UNIVERSIDAD DE LA RIOJA

TRABAJO FIN DE ESTUDIOS

Título

Los Datos Personales en la Red y las Herramientas Publicitarias

Autor/es

MARÍA DÍEZ ARNÁIZ

Director/es

SERGIO CÁMARA LAPUENTE

Facultad

Facultad de Ciencias Empresariales

Titulación

Grado en Administración y Dirección de Empresas

Departamento

DERECHO

Curso académico

2017-18

Los Datos Personales en la Red y las Herramientas Publicitarias , de MARÍA DÍEZ ARNÁIZ
(publicada por la Universidad de La Rioja) se difunde bajo una Licencia Creative Commons Reconocimiento-NoComercial-SinObraDerivada 3.0 Unported.
Permisos que vayan más allá de lo cubierto por esta licencia pueden solicitarse a los titulares del copyright.

© El autor, 2018
© Universidad de La Rioja, 2018
publicaciones.unirioja.es
E-mail: publicaciones@unirioja.es

FACULTAD DE CIENCIAS EMPRESARIALES

TRABAJO FIN DE GRADO

LOS DATOS PERSONALES EN LA RED Y LAS HERRAMIENTAS PUBLICITARIAS

PERSONAL DATA ON THE INTERNET AND ADVERTISING TOOLS

Autor: Dª. MARÍA DÍEZ ARNÁIZ

Tutor: Prof. D. SERGIO CÁMARA LAPUENTE

GRADO EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS

CURSO ACADÉMICO 2017-2018

Contenido

I.- RESUMEN/ABSTRACT

Resumen

La recogida, tratamiento y uso de los datos personales de los usuarios de Internet es una de las realidades que caracterizan el s. XXI. Desde el desarrollo de la tecnología, tanto de internet como del tratamiento de la información, ha surgido una preocupación del legislador por regular el control que el usuario puede tener sobre sus datos personales, especialmente los que se transmiten por Internet o las comunicaciones electrónicas. Las actividades que realizamos día a día implican el intercambio de datos personales, y ésta no siempre es voluntaria por parte de las personas. La gran cantidad de datos personales disponibles, unido al deseo de las empresas de usar esa información para diversos fines y los rápidos avances en la tecnología hacen que la regulación sobre los mecanismos que pueden usar las empresas quede pronto obsoleta e inaplicable.

Por ello, surge la necesidad de estudiar, desde un enfoque jurídico, cómo es la situación actual de la protección de datos personales, qué requisitos se les imponen a las empresas ante la recogida, tratamiento y cesión de esos datos personales, sobre todo en un contexto donde las empresas usan datos de sus propios clientes para transmitirles ofertas más personalizadas, obteniendo valor de dicha información.

Palabras clave: dato personal, consentimiento, cesión de datos personales, publicidad, *Cookies*, *Spam*.

The treatment, pick up and Internet users personal data management is one the 21th century main characteristics. Since the Internet was developed and information could start to be handled, a concern about the control of user personal data has appeared, especially data related to online transmissions or electronic communications. Day to day activities imply exchange of personal information, which is not always willing to be shared by most of the people. The amount of available network personal data, joined to the companies wish of using that information, and technology quick improvement, makes regulation to be soon out-dated, as much as not applicable.

Because of that, it arises the need of studying, from the legal point of view, how is the current state of personal data protection and which requirements are imposed to organizations before the pick up, treatment and transference of personal data, especially in a context where organizations use their own clients' data to show them more custom offers, gaining value from that information.

Keywords: Personal data, consent, transfer of personal data, publicity, Cookies, Spam.

1. Introducción

Si pensamos en un día normal de nuestra vida, nos encontramos con que el uso de la tecnología es una constante: nos levantamos con una alarma en el móvil, mientras desayunamos, hemos mirado el correo en el móvil (borrando todos esos mensajes de publicidad), leído el periódico online (que nos avisa de que instala *cookies* y que hay que deshabilitar los bloqueadores de publicidad) y respondido a los mensajes de *Whatssap*; haciendo deporte, nuestra pulsera ha monitorizado nuestra posición, ritmo cardiaco y las calorías que hemos gastado; al ir a comprar al supermercado, hemos usado los descuentos que nos envían por ser socios del club de la cadena; en casa, hemos usado uno de los servicios privados de televisión (*Netflix, HBO,* etc.) para ver una serie; hemos sacado las entradas del cine en el móvil; hemos respondido a una encuesta de *Google* al visitar el centro comercial; al ir a la universidad, hemos mirado la *app* del móvil o la web. Y mientras tanto, hemos compartido toda o parte de esta información en nuestras redes sociales. Valga como ejemplo sobre la cantidad de información que compartimos (ya sea de forma consciente, mediante redes sociales, o inconsciente) las palabras del fundador y CEO de *Facebook,* Mark Zuckerberg en 2010: "la privacidad ha muerto"[1].

Todas estas acciones, nuestra forma de usar la red y muchos de los servicios disponibles, hacen que estemos aportando información sobre nosotros mismos constantemente. El uso de la tecnología nos provee de datos importantes y útiles para la persona, pero también muy relevantes para las empresas: a través del uso de cupones o tarjetas de determinado comercio, ofrecemos información de qué, cuánto y cuándo compramos determinados productos; los terminales móviles transmiten información de geolocalización[2], que permiten saber dónde está una persona (y por ejemplo, enviarle una encuesta si ha visitado determinado comercio). Todo esto se enmarca en una de las características que definen este siglo, el uso de lo datos, lo que nos define como "Sociedad de la información": sociedad que se basa en la producción de servicios, especialmente aquellos en que se manipulan informaciones, y sobre el valor económico del conocimiento como recurso estratégico[3].

[1] PAGE, David; GARCÍA ALLER, Marta, "La privacidad no existe", *El Independiente,* 19 de febrero de 2017. En ella se cuenta el caso de una mujer que descubrió que su ex marido le era infiel viendo el recorrido que realizaba éste en la app UBER. También en el mismo artículo se preguntan por qué una *app* que sirve para que un niño dibuje animales pide permiso para saber la geolocalización y la agenda completa de contactos de determinado terminal.

[2] Se puede definir la geolocalización como "la aptitud para atribuir coordenadas geográficas a determinada información a través de herramientas informáticas", es decir, permite localizar tanto en el espacio como en determinado momento (temporal) un dispositivo. LÓPEZ JIMENEZ, D., CARLOS DITTMAR, E., "Internet móvil y geolocalización: nuevos retos para la privacidad en la era digital" VALERO TORRIJOS, J. (Coord.), *La protección de los Datos Personales en Internet ante la Innovación Tecnológica. Riesgos, Amenazas y respuestas desde la perspectiva jurídica*, Aranzadi, Pamplona, 2013, pág. 527.

[3] ROSSI CARLEO, L. "La sociedad de la Información: el ciudadano frente al poder de decisión ajeno" en LLÁCER MATACÁS, M.R., *Protección de datos personales en la sociedad de la información y la*

El uso que hacen las personas de la tecnología y el aprovechamiento que realizan las empresas de todos esos datos para mejorar la competitividad de sus productos o servicios hace que se produzcan situaciones en las que las organizaciones buscan, recaban y usan esos datos en su propio beneficio, vulnerando así los derechos de los usuarios. Por ello, a la vez que se produce el desarrollo de la informática en las últimas décadas del s. XX, que permiten la recolección y tratamiento de datos, aparece la preocupación sobre la pérdida de control sobre la información de los individuos[4]. Hoy en día, el "Gran Hermano" descrito por George Orwell en 1984[5], parece más posible que nunca, aunque no se sepa la identidad de esa mano que está detrás: si se trata de grandes multinacionales o el Estado[6].

Antes de comenzar con el desarrollo teórico que enmarca la protección de datos, parece pertinente destacar por qué las empresas buscan la información y la tratan. Actualmente, por el uso de la tecnologías *Big Data* los datos son transformados en conocimiento: los programas informáticos manipulan *Bits* y *Bytes* digitalmente (datos, como puede ser el número de veces que determinada persona va al supermercado), los ordenadores agrupan y manipulan esta información (así, saben cuántas veces se va al supermercado y, de media, cuánto gasta y en qué productos), transformando esos datos en información útil cuando son inteligibles para un humano (mediante informes), siendo conocimiento cuando se correlacionan informaciones entre sí[7]. Toda esta información, que se puede aplicar a millones de ejemplos, ha adquirido actualmente un valor[8], dando lugar al desarrollo de un nuevo modelo de negocio.

vigilancia, La Ley, Madrid, 2011, pág. 27. También, en un sentido que se enfoca menos a la importancia de la información, la sociedad de la información es "el conjunto de transformaciones sociales y económicas producidas como consecuencia del desarrollo exponencial y convergente de redes y servicios de telecomunicaciones, medios de comunicación y tecnologías de la información" en ORTEGA GIMÉNEZ, A., "La tutela del afectado ante los tratamientos ilícitos de sus datos personales desde la perspectiva internacional y su proyección en Internet" en VALERO TORRIJOS, J. (Coord.), *La protección de los Datos Personales en Internet ante la Innovación Tecnológica. Riesgos, Amenazas y respuestas desde la perspectiva jurídica*, Aranzadi, Pamplona, 2013, pág. 198, nota 3.

[4] GARRIGA DOMÍNGUEZ, A., *Nuevos retos para la Protección de datos personales*, Dykinson, Madrid, 2015, pág.90.

[5] Tratado también por la reciente serie *Black Mirror* en sus capítulos sobre redes sociales (donde la sociedad se basa en sistemas de puntuación de las personas, mediante implantes oculares y los teléfonos móviles: estas puntuaciones tienen influencia no solo en el perfil social de la gente, sino en aspectos socio económicos. Capítulo 8 temporada 3) o sobre las abejas (que usan la red social y los comentarios en la misma para eliminar personas, mediante la geolocalización, capítulo 13, temporada 3).

[6] Recordemos el escándalo que se produjo con las revelaciones de Edward Snowden sobre el espionaje de Estados Unidos, desveladas en 2013. Las noticias sobre el tema son interminables, pero baste mirar por ejemplo la noticia de CAMPBELL, Duncan, "Bajo la vigilancia de los Cinco Ojos" *El País*, 7 de julio de 2013.

[7] MORENO, J., "O valor económico da informação na sociedade em rede", Observatorio (OBS), Lisboa, nº 2, 2015, pág. 10.

[8] La determinación del valor económico exacto de la información es muy difícil por las características de la información: aislada de los soportes que la recogen, la información adquiere valor según se transforma

Así, la elaboración de bases de datos y registros personales se ha tornado imprescindible para las empresas. La imposibilidad de muchas de ellas de elaborar esas mismas bases de datos, o bien de tratar los datos para transformarlos en información útil ha posibilitado la creación de empresas dedicadas al almacenamiento, creación y tratamiento de bases de datos. Además, la demanda de las empresas de información sobre sus potenciales clientes ha hecho que muchas empresas piensen en "vender" datos que poseen. Aparecen así tres modelos de negocio diferentes que explotan los datos: las empresas relacionadas con la Web 2.0 (Vid. 2.1), el mercado publicitario y la industria de la inteligencia, policial y de la "seguridad"[9]. Sobre todo, y en lo que este a trabajo atañe, actualmente se han multiplicado las empresas que explotan la "inteligencia colectiva", es decir, datos que los usuarios comparten voluntariamente con otros usuarios (vía comunicaciones electrónicas, como *Whatssap,* vía redes sociales o comentarios en buscadores como Google).

El uso de los datos como fuente de ingresos, mediante su venta, tratamiento o recurso de valor informativo respecto a sus clientes, es el punto de partida en el que la protección de datos se mueve. La relevancia que los datos han adquirido para las empresas ha hecho que, en aras de obtener información, se vulneren los derechos del usuario, sobre todo en contextos en red, donde el movimiento de datos es inimaginable.

En este trabajo, se estudiarán las condiciones en las que los datos personales pueden ser recabados, tratados y usados, comenzando por perfilar los conceptos centrales del derecho a la protección de datos personales y también de las tecnologías que rodean a la recogida y tratamiento de los datos, que han permitido que las empresas puedan recabar y usar los datos de forma sencilla y barata. A continuación, se verá qué regulación está vigente sobre la protección de datos personales y las novedades que se han producido. Profundizando un poco más, se estudiará el principal requisito que han de cumplir las empresas para tratar datos personales (el consentimiento). Por último, se centrará este estudio en las herramientas que se utilizan para la recogida de datos y sus condiciones para ser legales, las *cookies,* y bajo qué términos es lícita la cesión de datos personales, acabando con la relación que puede tener el derecho de protección de los datos personales y una herramienta publicitaria del día a día, el *Spam.* La metodología para realizar este trabajo adopta un enfoque jurídico, por lo que será el formato que se adopte a la hora de realizar las referencias y citas.

2.- Conceptos: la revolución digital.

Una vez se acepta que Internet es una necesidad del día a día, omnipresente y, casi, imprescindible, se deben afrontar los retos que su uso conlleva. En el ámbito de la

o trata, y depende de la capacidad que esta información tenga o no para ser conocida por un grupo más o menos reducido de entidades. En MORENO, J., *op. cit.* pág. 12

[9] MAROTO CALATAYUD, M., "Redes sociales en Internet y "*Data mining*" en la prospección e investigación de comportamientos delictivos" en RALLO LOMARTE, A., MARTÍNEZ MARTÍNEZ, R., *Derecho y Redes sociales,* Civitas, 2010, pág. 218.

protección de datos y, centrándonos en los servicios, es importante delimitar todos los elementos, tanto jurídicos como tecnológicos, que van a conformar el marco en el que los usuarios se mueven, y dónde se encuentran sus derechos y obligaciones. Las nuevas tecnologías suponen escenarios novedosos en la recogida y tratamiento de los datos, que estudiaremos primero. Luego, realizaremos una aproximación a la definición de dato personal, que ha ido evolucionando con la tecnología.

2.1.- Servicios en Internet y su interacción con *Big Data* y *Cloud Computing*.

Así, ¿qué entendemos por Servicios de la sociedad de la información? La primera definición la podemos encontrar en la Directiva 2000/31/CE de 8 de junio de 2000, "relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior" (a partir de ahora, Directiva sobre el Comercio Electrónico), que en su artículo 2.a. indica que se entiende cualquier servicio prestado que tenga las siguientes características: normalmente a cambio de una remuneración, a distancia, por vía electrónica, a petición individual de un destinatario del servicio.

Aunque puede parecer que esta definición deja fuera aquellos servicios "gratuitos", hay que tener en cuenta que un servicio no remunerado por el usuario puede ser también un servicio de la sociedad de la información sí implica una actividad económica para quien lo presta[10], sobre ello se pronuncia el párrafo segundo del apartado a del anexo de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio electrónico, en su anexo (en adelante, LSSICE), añadiendo a la definición anterior el siguiente matiz: "El concepto de servicio de la sociedad de la información comprende también los servicios no remunerados por sus destinatarios, en la medida en que constituyan una actividad económica para el prestador de servicios" (sobre esta gratuidad de los servicios volveremos más adelante). Además, hemos de tener en cuenta que el matiz incluido por la característica de "a distancia" hace referencia al uso de internet y la web 2.0[11]. Aunque la definición no deja claro qué tipo de servicios podemos encontrar, LSSICE proporciona en su anexo una relación de ejemplos:

[10] PEGUERA POCH, M., "Servicios de la Sociedad de la Información" en PEGUERA POCH, M. (Coordinador), *Derecho y Nuevas Tecnologías*, Ed. UOC, Barcelona, 2005, págs. 146-147. En el mismo sentido se pronuncia la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio electrónico, en su anexo, añadiendo a la definición anterior el siguiente matiz: "El concepto de servicio de la sociedad de la información comprende también los servicios no remunerados por sus destinatarios, en la medida en que constituyan una actividad económica para el prestador de servicios".

[11] La evolución de la web convencional puede ser definida como "serie de aplicaciones y páginas de internet que, a través de sistemas de inteligencia colectiva, proporcionan servicios interactivos en la red, y que en su conjunto integran la segunda generación de la *world wide web*. A diferencia de la web 1.0, que estaba integrada por páginas estáticas programadas, en las que solo se podía acceder a la información que en ellas

1º. La contratación de bienes o servicios por vía electrónica.
2º. La organización y gestión de subastas por medios electrónicos o de mercados y centros comerciales virtuales.
3º. La gestión de compras en la red por grupos de personas.
4º. El envío de comunicaciones electrónicas.
5º. El suministro de información por vía telemática.
6º. El vídeo bajo demanda, como servicio en que el usuario puede seleccionar a través de la red, tanto el programa deseado como el momento de su suministro y recepción, y, en general, la distribución de contenidos previa petición individual.

Como se puede observar, los servicios aportados por aplicaciones de mensajería como *Whatsapp* o *Hotmail*, incluidas en el ejemplo relativo al envío de comunicaciones electrónicas, entran en la categoría de servicios de la información. Sin embargo, ¿qué une a los nuevos servicios que internet nos ofrece con la protección de datos personales? A priori, un servicio en el que dos usuarios tengan una conversación no tiene por qué implicar una transmisión de datos más allá de los transmitidos entre los usuarios (conversaciones privadas) y los llamados datos de tráfico[12]. Así es como aparece el *Big Data*, concepto con el que nos referimos a dos realidades: de un lado, la enorme cantidad de datos o información disponibles en la actualidad que no puede ser procesada o analizada utilizando herramientas o procesos tradicionales[13], de otro, nos referimos al conjunto de herramientas y sistemas informáticos que analizan los datos buscando patrones recurrentes y correlaciones dentro del conjunto de aquellos[14]. Todos los mensajes, ya sea en forma de texto, vídeo o imagen, o los datos de tráfico de la conversación, contienen información que puede ser procesada mediante las nuevas técnicas, que permiten obtener conocimiento de ciertos datos que, de forma aislada, no significarían nada.

De todo ello ha nacido lo que se conoce como *Data mining* (o la minería de datos): comercio que se sirve de determinados programas (*Big Data)* para rentabilizar, mediante

se ofrecía (y actuaba como medio de comunicación)". Se puede incluir en ella todas aquellas páginas en las que el usuario genera contenido: Google, Flickr, Twitter, Facebook, YouTube, etc. En SIMÓN CASTELLANO, P., *El régimen constitucional del derecho al olvido digital,* Tirant lo Blanch, Valencia, 2012, pág. 24.

[12] "Son datos que se generan en el curso de una comunicación pero que no aluden al contenido comunicado, sino a algunos aspectos accesorios de la propia comunicación efectuada, como serían los referidos a su existencia, su origen y destino, el medio utilizado para realizarla o su duración" en GALÁN MUÑOZ, A., "¿Nuevos riesgos, viejas respuestas? Estudio sobre la protección penal de los datos de carácter personal ante las nuevas tecnologías de la información y la comunicación", en GALÁN MUÑOZ, A. (Coord.), La *protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y comunicación,* Tirant lo Blanch, Valencia, 2014, pág. 258-259.

[13] GIL GONZÁLEZ, E., *Big Data, privacidad y protección de datos*, Agencia Española de Protección de Datos, Madrid, 2016, pág. 18.

[14] GARRIGA DOMÍNGUEZ, *op. cit.* pág. 28.

el análisis de datos, ciertos servicios[15], como pueden ser los servicios de correo electrónico, periódicos on-line, etc., en los que de una u otra forma pueden hacerse con datos relevantes en cuanto a consumo, preferencias, gustos o clics.

Hay que tener en cuenta que algunos servicios (como *Whatsapp* o *Hotmail*) se basan en la tecnología de *Cloud Computing:* "un modelo que permite el acceso a la carta o bajo demanda a todo un conjunto de recursos informáticos como aplicaciones, infraestructura, datos u otros servicios como por ejemplo el almacenamiento de información o el procesamiento de datos recogidos con un mínimo de esfuerzo o de interacción con el proveedor del servicio"[16]. Es decir, todos los datos que los usuarios generan no se guardan en sus terminales, sino que usan servidores externos, debido a que la ingente cantidad de información que se genera hace imposible guardarlos en las memorias ordinarias de los ordenadores o los *smartphones.*

Así, comenzamos a ver el inicio del problema: el uso de servicios que tienen internet como medio, el hecho de que nuestra información no se guarda en nuestros terminales, unido a la aparición de un comercio sobre los datos forman el cóctel perfecto para que determinada información que los usuarios creen suya termine siendo usada en beneficio de otros.

2.2.- Dato personal.

Determinado el ámbito en el que nos vamos a mover respecto a la protección, nos queda saber qué es un dato personal. La definición de "dato personal" puede encontrarse en las diferentes leyes que regulan la protección de datos de forma similar: "toda información sobre una persona física identificada o identificable"[17]. Nos encontramos con varios problemas con esta definición tan amplia: el avance de la tecnología ha hecho evolucionar

[15] El *Data mining* puede ser definido como "el negocio en el que junto a […] proveedores intervienen tanto entidades públicas como privadas, que están dispuestas a pagar importantes cantidades de dinero con tal de acceder a ellos, para después poder procesarlos con los fines más diversos, desde elaborar perfiles de consumidores para realizar publicidad personalizada o contextualizada, hasta efectuar pronósticos de criminalidad de los sujetos a los que los datos están referidos" según GALÁN MUÑOZ, A. *op. cit.* pág. 256.

[16] Definición del NSIT (*National Institute of Standards and Technologies* del Departamento de comercio del gobierno federal de los Estados Unidos) recogida en NAVAS NAVARRO, S., "Computación en la nube: Big Data y protección de datos personales", Indret (Revista para el Análisis del Derecho), Barcelona, nº4, 2015, pág. 9.

[17] Esta definición puede encontrarse en el Reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (a partir de ahora, nuevo Reglamento de datos personales) en su artículo 4, del mismo modo que aparece definido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal (a partir de ahora LOPD): "cualquier información concerniente a personas físicas identificadas o identificables" (art. 3).

la capacidad para hacer identificable a una persona a partir de datos que, de forma aislada, no comportarían información suficiente para señalarla; de otro lado, hemos de saber si la información recogida por determinados programas (como las *cookies*) o determinada información que se puede extraer de nuestros *clics* realizados del correo electrónico son abarcados por la definición.

2.2.1.- "Persona identificable o identificada".

La legislación supedita la protección de datos personales a que éstos permitan la identificación directa sin necesidad de tratamiento (identificada) o potencial (identificable). La identificación es, así, un elemento esencial del derecho a la protección de datos[18]. El art. 4, 1 del nuevo Reglamento de datos personales indica que una persona es considerada identificable si su: "identidad puede determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona"[19].

Un requisito que las normas[20] imponen a la identificación, o potencial identificación, de la persona es que ésta no requiera un plazo o actividad desproporcionados, con indiferencia de la complejidad de la operación que nos conduzca a la personalización concreta[21].

Tradicionalmente, el nombre y los apellidos han sido el identificador generalmente reconocido, pero existen muchos más datos que permiten la identificación directa de una persona, como pueden ser, entre otros, el Documento Nacional de Identidad, un código Pin, el número de abonado a un servicio o determinadas partes del cuerpo humano que actúan como datos biométricos (como la huella, los rasgos faciales o el iris), etc.[22] Sin embargo, el uso de las nuevas tecnologías y, sobre todo, del *Big Data*, permiten la identificación mediante otro tipo de datos. Todas esas consideraciones son tenidas en

[18]LLÁCER MATACÁS, M.R., *La autorización al tratamiento de información personal en la contratación de bienes y servicios,* Dykinson, Madrid, 2012, pág. 24 y VALERO TORRIJOS, J., "Las quiebras en Internet de la regulación legal del derecho a la protección de los datos de carácter personal: la necesaria superación de un modelo desfasado" en VALERO TORRIJOS, J.*, La Protección de los Datos…,* cit.., pág. 42.

[19] Aunque el legislador español no define en la LOPD qué es una persona identificada o identificable, sí lo hace el Reglamento de desarrollo de la LOPD en su artículo 5.1. o y la Directiva 95/46/CE, sobre Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y la Libre Circulación de estos datos (A partir de ahora DPD-95) en su art. 2.a.

[20] Art. 5 apartado o del Real Decreto 1720/20017, de 21 de diciembre, de desarrollo de la LOPD y del mismo modo el Considerando 26 de la DPD-95. Este matiz, sin embargo, no se incluye en el RPD-2016-

[21] GARRIGA DOMÍNGUEZ*, op. cit. 167.*

[22] LLÁCER MATACÁS, M.R., *La autorización al… cit.* pág. 24.

cuenta por el nuevo Reglamento de datos personales, de tal forma que el compendio de tipo de datos que recoge como potenciales identificadores de una persona es muy amplio. Y es que las nuevas tecnologías permiten la identificación a través de datos como por ejemplo coordenadas geográficas: la transmisión de la geolocalización que recogen los teléfonos móviles, u otros elementos como pueden ser los relojes inteligentes (*smartwatch),* permiten saber datos de la persona como por ejemplo dónde vive, dónde trabaja, o si está o no en casa.

Este requisito adquiere una singular perspectiva en el caso de Internet, por lo que se refiere fundamentalmente a dos instrumentos esenciales: la dirección IP y el correo electrónico. En cuanto a la primera, el principal problema de este número identificativo otorgado por el proveedor de servicios es que puede ser tanto estático como dinámico. En el primer caso, el ordenador siempre tiene asignado el mismo número, mientras que, en la segunda, esa información varía de forma aleatoria. Sin embargo, ante ambas informaciones, hay que tener en cuenta que la identificación de la IP con determinada persona contratante solo es posible para el prestador del servicio de acceso a Internet (por lo que para él sí constituiría un dato personal), pero no para terceros ajenos a la prestación del servicio. A todo ello hay que añadir que el proveedor tiene asignada una IP a determinada persona contratante, que no tiene por qué ser el usuario del ordenador en cuestión[23], por lo que aún se hace más difícil identificar a la persona correcta que hace uso en cada momento de internet (si no es con un proceso enrevesado y largo de investigación).

Más complejo resulta el caso de los correos electrónicos. La Agencia Española de Protección de datos (AEDP) estableció en su informe 2007/0391 que aquéllos que contengan datos significativos en la dirección de correo electrónico (como nombre y apellidos, empresa u organización a la que se pertenece), se consideraría un dato personal[24]. Un ejemplo de ello podría ser los correos electrónicos de la Universidad de La Rioja, que se componen de un acrónimo de los nombres y apellidos. Sin embargo, no es desconocido que la mayoría de correos electrónicos no institucionales permiten una combinación de letras y números que pueden perfectamente no corresponder con una identificación, sin que sea necesario ni siquiera informar al prestador de tales servicios de una identificación fidedigna[25]. Sólo en el caso de que el proveedor obligara a dicha identificación, tendríamos la misma consideración a realizar que con la dirección IP: sería posible la identificación de la persona por parte del proveedor, para el cual sí que serían

[23] VALERO TORRIJOS, *op. cit.* 43.

[24] Informe jurídico 0391/2007, de la Agencia de protección de datos, pág. 1-3. Glosado en PANIZA FULLANA, A., "Protección de datos, *cookies* y otros instrumentos de navegación" en FERNÁNDEZ LÓPEZ, J.M., *Publicidad, Defensa de la Competencia y Protección de datos*, Thomson Reuters, Pamplona, 2010, pág. 40

[25] VALERO TORRIJOS, *op. cit.* pág. 45.

datos personales, pero no para terceros ajenos a la relación contractual. En el resto de los casos (relación alfanumérica más o menos aleatoria), según la AEDP se estará a la normativa general: siempre que la identificación no suponga un "*esfuerzo desproporcionado" [26]*.

Sin embargo, se produce en la actualidad una revisión de la definición de dato personal en cuanto a su requisito de identificabilidad: en un entorno como internet, donde las posibilidades de anonimato son muy relevantes, este requisito puede haber quedado obsoleto[27]. Pensemos por ejemplo en las *cookies*[28] instaladas en un ordenador: le es indiferente quién sea el usuario, sea el contratante de la línea de internet o un mero usuario de ese ordenador o terminal, el programa recoge los datos para crear perfiles y remitir luego publicidad[29](ya sea mediante *banners*[30] personalizados o *spam*[31]). O bien en la tecnología RFID[32], en la que ciertas etiquetas o elementos permiten el seguimiento de los consumidores, por ejemplo, en un supermercado: es indiferente quién sea ese consumidor, utilizan esa información para averiguar el comportamiento del mismo y aplicarlo a sus técnicas de venta. El requisito de la identificabilidad ha pasado a ser secundario sin por ello dejar de lado para este tipo de datos cierta protección para el usuario: que sea

[26] "Incluso en los casos en que no hay datos identificables de una persona, según la Agencia de Protección de Datos, afirma que la dirección aparecerá referenciada a un dominio concreto, de tal forma que podría identificarse acudiendo al servidor en que se gestione dicho dominio", en PANIZA FULLANA, "Protección de datos, *cookies…".* cit. pág. 40. Se prueba así que los requisitos de no desproporcionalidad (establecidos en Art. 5 apartado o del Real Decreto 1720/20017, de 21 de diciembre, de desarrollo de la LOPD y del mismo modo el Considerando 26 de la DPD-95), dependen del punto de vista.

[27] VALERO TORRIJOS, *op. cit.* pág. 42.

[28] Las *cookies* son, técnicamente: "cadenas de información alfanumérica formadas por diferentes campos específicos que serán depositadas por el servidor en el disco duro del cliente durante una visita del mismo" según PANIZA FULLANA, A., "Protección de datos, *cookies…".* cit. 26. Es decir, son programas que se instalan en los ordenadores al visitar determinada página o al hacer clic en determinado enlace. Estas pueden ser anónimas, de tal forma que no identifiquen al usuario, o identificadas (lo que más adelante resultará muy relevante, vid. 5.1).

[29] LLÁCER MATACÁS, M.R., *La autorización al… cit.* pág. 28.

[30] Definidos como "programa informático con finalidad publicitaria que consiste en gráficos, imágenes, textos, normalmente formando una combinación de todos o algunos de dichos elementos, que permite guiar al navegante o usuario de la Red hasta la página o el sitio de un anunciante, donde éste da a conocer de una forma más detallada sus productos o servicios" en VEGA VEGA, J.A., *Contratos electrónicos y protección de los consumidores,* Editorial Reus, Madrid, 2015, pág. 167.

[31] "Se entiende por *spam* toda aquella comunicación publicitaria no solicitada (que, normalmente, tiene como fin ofertar, comercializar o tratar de despertar el interés de un determinado producto, servicio y/o empresa) que llegue tanto al buzón de correo electrónico […] como a otros espacios diversos" en LÓPEZ JIMÉNEZ, D., "El denominado *bluespam*: incidencia sobre la privacidad del destinatario" en VALERO TORRIJOS, J. (Coord.), *La Protección de los Datos …,* cit. pág. 495.

[32] Esta tecnología es definida por LLÁCER MATACÁS como aquella que permite la recogida de datos a distancia y puede, mediante el tratamiento de los datos, prever los desplazamientos de los consumidores. Son las llamadas etiquetas inteligentes, que pueden implantarse en cualquier objeto o embalaje, y que se comunican con un dispositivo fijo o móvil. COLIN, C., PULLET, Y., "Sociedad de la información y Marketing: *case* study" en LLÁCER MATACÁS, M.R., *Protección de datos personales…* cit. pág. 231.

indiferente su identificación no debe significar que dejen de recabar mi consentimiento, cuando esa información puede tener futuras consecuencias para mí (por ejemplo, el envío de publicidad, o de ofertas personalizadas del supermercado).

Por ello, se ha producido una evolución del concepto, que el Grupo de Trabajo del art. 29 (en adelante, GT 29)[33], plasmó en su Opinión 4/2007: el término "dato se refiere a una persona si hace referencia a su identidad, sus características o su comportamiento o si esta información se utiliza para determinar o influir en la manera en que se la trata o se la evalúa", aunque con esta definición surgen problemas claros con los derechos de acceso, rectificación o cancelación de los mismos (que se verá más adelante) o la posibilidad de consentimiento[34]. También la AEPD aporta una nueva perspectiva al concepto en su *Contribución de la AEPD a la Consulta de la Comisión sobre un enfoque global de la protección de datos personales en la Unión Europea:* "Sería deseable que la definición de "datos personales" sea lo suficientemente amplia para anticiparse a las posibles evoluciones y cubrir todas las "zonas grises" existentes en su ámbito de aplicación […]. Por tanto, el concepto de dato personal debería cubrir aquellas situaciones en las que se desconoce el nombre del sujeto, pero se tiene un perfil completo sobre él"[35].

Estas nuevas perspectivas del concepto de dato personal se centran más en la posibilidad de definir a un individuo de forma completa y con consecuencias para el mismo, no tanto en identificarlo de forma objetiva, para evitar posibles lagunas ante los avances de las nuevas tecnologías, aunque sin dejar de lado la tradicional identificación que sí se produce en otros ámbitos.

2.2.2.- "Cualquier información".

El acierto del legislador en esta materia consiste en adoptar en la definición de dato personal un concepto abierto en cuanto a la tipología, que no se centre en listas cerradas o casuísticas que puedan crear problemas, sobre todo, con las nuevas tecnologías[36]. El concepto de dato es muy similar tanto en la LOPD, en la DPD y en el nuevo reglamento, aunque no aparece definido, puede asimilarse con cualquier información, al margen de qué formato presente. En el Reglamento de desarrollo de la LOPJ[37], en su artículo 5, sí realiza una enumeración que parece referirse al tipo de formato de la información, aunque

[33] *vid. Infra* epígrafe 3.1. B.
[34] LLÁCER MATACÁS, M.R., *La autorización al… cit.* pág. 29.
[35] GARCÍA PÉREZ, R.M., "La protección de datos de carácter personal del Consumidor en el Mercado Único Digital", *Revista de Derecho Mercantil*, julio-septiembre 2016, pág. 207, nota 18.
[36] Así lo sostienen MESSÍA DE LA CERDA BALLESTEROS, J.A., *La cesión o comunicación de datos de carácter personal*, Thomson Civitas, Madrid, 2003, pág. 28 y VEGA VEGA, J.A., *op. cit.* pág. 365.
[37] Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

de nuevo no cerrada: cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo.

Esta definición amplia quiere evitar que, del tratamiento de un conjunto de datos aparentemente irrelevantes (sean del tipo que sean) se consigan datos que permitan la identificación de una persona concreta[38].

Si desde el punto de vista de su *contenido*, el término dato se refiere así de forma amplia a todo tipo de información, desde el punto de vista de su *naturaleza*, el concepto de dato incluye tanto datos objetivos (números identificativos, o determinada presencia de una sustancia en sangre) como subjetivos (que pueden darse en ámbitos como el bancario, determinando la fiabilidad o no de un cliente; en el de seguros, indicando si una persona puede morir pronto por determinada enfermedad). Además, se ha de tener en cuenta que para que la información quede protegida por las normas no es necesario que sea verídica o esté probada. [39].

Especial mención requiere el hecho de que sí que hay un grupo de datos que merecen protección añadida por su contenido, los llamados datos sensibles. La Directiva 95/46/CE (así como la LOPD en su artículo 7, como "Datos especialmente protegidos") conceptúa como tales en su artículo 8 los datos que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de datos relativos a la salud o a la sexualidad. Por su parte, el Reglamento de datos personales (nuevo reglamento de 2016) añade a estas categorías los datos genéticos, y los datos biométricos (art. 9). Estos datos requieren de mayor protección, aunque en la legislación se incluyen asimismo ciertas excepciones, por las que sí pueden tratarse dichos datos (como puede ser el consentimiento explícito, o el tratamiento por asociaciones especialmente vinculadas como son partidos políticos o asociaciones relacionadas con el origen).

3.- Marco jurídico. Hacia un nuevo modelo de protección de datos

Hablar de marco normativo cuando se hace referencia a las nuevas tecnologías siempre es difícil: el avance vertiginoso de la tecnología deja muy pronto al derecho obsoleto e inaplicable[40] a nuevas situaciones que la realidad tecnológica crea. Asimismo, hay que tener en cuenta el carácter global de los servicios a los que nos referimos, hace aún más

[38] MESSÍA DE LA CERDA BALLESTEROS, J.A., *op. cit.* pág. 28.
[39] GIL, E., *Big Data, privacidad…,* cit. pág. 46.
[40] DRUMMOND, V., *Internet, privacidad y datos personales*, Ed. Reus, Madrid, 2009, pág. 66. Y SCHÜTZ, P., "The Set up of Data Protection Authorities as a New Regulatory Approach" en GUTWIRTH, S., LEENES, R., DE HERT, P., POULLET, Y. (Editors), *European Data Protection: In Good Health?* Springer, London, 2012, pág. 127.

compleja la regulación de la protección de datos en estas transacciones, que ha de tener en cuenta las diferentes localizaciones de los prestadores de los servicios y sus usuarios, y las posibles incompatibilidades entre las diferentes legislaciones de los países.

Como se expresaba anteriormente, el uso de la tecnología *Big Data* permite el procesamiento de datos que, aun inconexos en origen, permiten obtener información relevante de las personas mediante su tratamiento que permite la re-identificación de los sujetos. Ello supone sin duda cierto poder para las empresas, que pueden lesionar los derechos de los usuarios de internet[41]. Esto es especialmente relevante en el proceso normativo, por la presión de los *lobbies* tecnológicos de las empresas líderes de la red (*Google, Microsoft, Amazon, Facebook…*)[42].

La regulación de la protección de las personas que a continuación se expondrá tiene una doble vertiente en Internet: de un lado, la normativa sobre protección de datos, de otro, la regulación que rodea el contexto tecnológico y empresarial en el que nos movemos. Esta normativa pretende devolver al usuario el control sobre sus datos personales, uso y destino, con el propósito de impedir su tráfico ilícito y lesivo, en cualquier etapa: su recogida, tratamiento y almacenamiento, o bien su posible cesión a terceros[43].

3.1.- Protección de datos personales.

3.1.1.- Dicotomía internacional.

La ausencia de fronteras en la circulación de datos en Internet provoca, como hemos indicado, que se difuminen los sistemas legales que regulan la privacidad. El gran problema llega con las grandes corporaciones internacionales que, aunque operan en los Estados miembros y son responsables del tratamiento de datos personales, no tienen sede en la Unión Europea[44]. Y es que nos encontramos a escala internacional con dos sistemas totalmente distintos referidos a la tutela de datos personales: el estadounidense, mucho

[41] REBOLLO DELGADO, L., "Protección de datos (I): Origen, Justificación de su necesidad y regulación en Europa", en REBOLLO DELGADO, L., GÓMEZ SÁNCHEZ, Y., *Biomedicina y Protección de Datos*, Dykinson, Madrid, 2009, pág. 129.

[42] GARCÍA PÉREZ, R.M., *op. cit.* pág. 205.

[43] VEGA CLEMENTE, V., "Comercio electrónico y protección de datos", *Revista de Estudios Económicos y Empresariales*, nº 22, 2010, pág. 208.

[44] De hecho, en los países anglosajones se considera que un país es menos competitivo en el sector de la información cuánto más rígida es su legislación sobre protección de datos. En respuesta a esta creencia y sus normas autorreguladoras, la Unión Europea estableció la normativa de protección de datos. En VILASAU SOLANA, M., "Derecho a la intimidad y protección de datos personales" en PEGUERA POCH, M., *Derecho…,* cit. pág. 95.

más permisivo y liberal, y el europeo, más sensible a la protección de la intimidad y datos personales[45].

Para comprender la problemática, hay que entender que el sistema en Estados Unidos (principal sede de entidades titulares de redes sociales, aplicaciones informáticas, etc.)[46] es totalmente distinto al europeo. Y es que Estados Unidos es el país con menos garantía en la protección de los datos personales, puesto que priman el derecho al comercio de datos por parte de las empresas antes que la protección de datos del consumidor o usuario, dejando a merced de la autorregulación la vía de control[47], que lleva a garantizar la privacidad incluso mediante empresas emisoras de certificados (como muestra para la confianza de los usuarios)[48].

A nivel internacional, sí hay ciertas entidades que se han esforzado por avanzar en la protección de datos. De un lado, las Directrices de la OCDE (Organización para la Cooperación y el Desarrollo Económicos) que buscan establecer unas reglas básicas reguladoras del Derecho que, adoptadas de forma uniforme puedan garantizar la inexistencia de obstáculos a la transferencia internacional de datos[49]. A estas se unen las Directrices de las Naciones Unidas, contenidas en la Resolución A/RES/45/95 de la Asamblea General de las Naciones Unidas, de 14 de diciembre de 1990, sobre Principios rectores sobre la reglamentación de los ficheros computadorizados de datos personales, que pretendió de la misma manera crear una lista mínima de principios de protección de datos (aunque se circunscribe únicamente a los tratamientos automatizados).

3.1.2.- La Unión Europea: nuevo Reglamento.

La preocupación en la Unión Europea por la protección de datos tiene su origen hace décadas (siendo el primer texto normativo de la materia el Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal de 28 de enero de 1981, que es el referente principal de una serie de intentos que comienzan en 1967), con especial inquietud por la falta de armonización y homogeneización de las normas nacionales sobre la materia. El desarrollo del proceso

[45] VEGA VEGA, J.A., *op. cit.* pág. 359.
[46] GARCÍA PÉREZ, R.M., *op. cit.* pág. 216.
[47] Se parte de la idea de que la primera enmienda protege el comercio de los datos de carácter personal y, además, considera que su uso en el espacio público es algo que beneficia a todos. GALÁN MUÑOZ, A. *op. cit.* pág. 247-248.
[48] DRUMMOND, V., op. *cit.* pág. 77.
[49] PUENTE ESCOBAR, A., "Breve descripción de la evolución histórica y del marco normativo internacional del Derecho fundamental a la Protección de Datos de carácter personal" en PIÑAR MAÑAS, J.L. (Coord.), *Protección de datos de carácter personal en Iberoamérica (II Encuentro Iberoamericano de Protección de datos, La Antigua-Guatemala, 2-6 de junio de 2003),* Tirant lo Blanch, Valencia, 2005, pág. 51-53.

europeo, culminado con los derechos a la libre circulación de personas, capitales y, por supuesto, información, hizo necesario un desarrollo normativo sobre la protección de los datos que unificara las legislaciones de los países miembros.

Tras el Convenio 108, en lo relativo a datos personales y personas físicas, el siguiente gran paso es la publicación de la Directiva 95/46/CE, de 24 de octubre de 1995, relativa a la protección de personas físicas en lo referido al tratamiento de datos personales y su libre circulación (DPD). Esta directiva que, si bien realiza la primera unificación legislativa y es la base junto con el Convenio 108 de la posterior normativa de protección de datos, adolece de una indefinición jurídica de la mayoría de conceptos utilizados[50]. Sin embargo, hay que tener en cuenta que, en este momento, el uso de internet no estaba generalizado, y los fallos de la directiva se reconocerán por la evolución de la tecnología[51].

Sin embargo, aunque el esfuerzo normativo fue muy importante hasta la publicación de la Directiva 95/46, no hay una actualización jurídica hasta la actualidad. No será hasta 2016 cuando se publique al fin el Reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante RGPD), que entrará en vigor el 25 de mayo de 2018 (los dos años entre su publicación y su entrada en vigor pretende dar tiempo a los países miembros a adaptar sus normativas internas[52]). En este centraremos nuestro estudio (sobre todo del consentimiento *vid.* Apartado 4)

En el mismo año se publicó también la Directiva 2016/680, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, sobre la transmisión de datos para cuestiones judiciales y penales[53] que, al pertenecer al ámbito administrativo, no se estudiará.

[50] REBOLLO DELGADO, L., *Biomedicina y protección…. cit.* pág. 139-140.

[51] GIL GONZÁLEZ, E., "*Big data* y datos personales: ¿es el consentimiento la mejor manera de proteger nuestros datos?, Diario la Ley, Nº 9050, 2017, pág. 6.

[52] Hay que puntualizar que si bien un Reglamento europeo no deroga la legislación nacional, sí que existe un principio de primacía del Derecho comunitario: el Reglamento desplaza a las legislaciones nacionales en su aplicación, por lo que ante conflictos entre ambas normas (cuando ante la misma situación la norma nacional es contraria al Reglamento), primará siempre el Reglamento. Sin embargo, sí que deroga la Directiva 95/46.

[53]Directiva 2016/680, del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

Al margen de las directivas y reglamentos propios de protección de datos personales, existen otras fuentes normativas que, si bien no son específicas de protección de datos, sí se refieren en sus textos a algunos aspectos, como pueden ser:

- Directiva relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones[54], que tiene como propósito establecer obligaciones y derechos tanto de abonados como de proveedores, en el ámbito de las telecomunicaciones y, por tanto, respecto de los datos personales que se traten en el ámbito (limitando por ejemplo los datos personales en guías impresas o electrónicas accesibles al público)[55].

- Directiva sobre privacidad y comunicaciones comerciales[56], que tutela de forma especial los derechos como usuarios de las personas físicas y jurídicas en las comunicaciones electrónicas[57].

- Directiva sobre la conservación de datos generados con la prestación de servicios de comunicaciones electrónicas[58]. Esta directiva introduce importantes novedades a propósito del tratamiento de datos personales de tráfico y localización generados por el uso de servicios de comunicaciones electrónicas, ya que suponen una herramienta muy valiosa en la prevención, investigación, detección y enjuiciamiento de delitos, en especial contra la delincuencia organizada[59].

Además de las directivas y reglamentos europeos, actualmente hay que tener en cuenta los documentos publicados por el GT 29. Éste es un órgano consultivo creado por la DPD[60], que integra a todas las autoridades de protección de datos de los Estados miembros. Los documentos que publica no son vinculantes, pero tienen un importante valor doctrinal y son citados frecuentemente por investigadores, legisladores y tribunales[61].

[54] Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.
[55] REBOLLO DELGADO, L., *Biomedicina y protección…. cit.* pág. 140.
[56] Directiva 2002/58/CE, de 12 de julio de 2002, sobre privacidad y comunicaciones comerciales, en adelante Directiva sobre privacidad y comunicaciones comerciales. .
[57] HERRÁN ORTIZ, A., "La protección de datos personales de los consumidores y usuarios en los servicios de comunicaciones electrónicas" en CANEDO ARRILLAGA, M.P. (Coord.), *Derecho del Consumo: Actas del Congreso Internacional sobre Derecho de Consumo,* Tirant lo Blanch, Valencia, 2009, pág. 609.
[58] Directiva 2006/24/CE, de 15 de marzo de 2006, sobre la conservación de datos generados con la prestación de servicios de comunicaciones electrónicas
[59] HERRÁN ORTIZ, A., *op. cit.* 614.
[60] Artículo 29 de la DPD. En el art. 28 se conmina a los estados a crear una autoridad de control, que se reflejaría en España en la creación de la AEDP.
[61] GIL GONZÁLEZ, E., *Big Data, privacidad…,* cit. Pág. 51.

Sin embargo, ¿qué pasa cuando la empresa se encuentra, por ejemplo, en Estados Unidos, país con una política de protección de datos totalmente distinta a la nuestra? Este problema se resuelve en la Unión Europea con las reglas especiales sobre la aplicación extraterritorial del derecho de protección de datos: por la situación geográfica de los medios usados para el tratamiento (art. 4.1 letra c de la Directiva 95/46/CE) por lo que se aplicará la ley del estado donde éstos se encuentren. El grupo de trabajo del art. 29 (a partir de ahora, GT 29) ha considerado que la instalación de *cookies* en el equipo terminal de un usuario con el objeto de recabar información entra dentro del supuesto, aplicándose así la ley nacional del Estado miembro donde se encuentre el ordenador del usuario donde el programa se hubiera instalado[62]. Así, este precepto pretende evitar que las grandes corporaciones usen la deslocalización para no cumplir la regulación sobre datos personales. En la nueva regulación, el Reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 (RGPD que entrará en vigor en mayo de 2018), la normativa europea será aplicable a aquellos responsables de tratamientos que, aún no teniendo un establecimiento en Europa, dirijan sus ofertas de bienes o servicios a ciudadanos de la Unión, independientemente de que requiera el pago o no de contraprestación o monitoricen sus conductas (art. 3).

3.1.3.- España ¿Nuevos problemas, viejas soluciones?

La publicación en 1995 de la Directiva 95/46/CE obliga a los estados miembros, y entre ellos España, a la renovación de la legislación sobre datos personales. Anteriormente, regulaba la protección de datos personales la Ley Orgánica 5/1992 de 29 de octubre de Regulación del Tratamiento Automatizado de Datos de Carácter Personal (LORTAD), que respondía al mandato contenido en el art. 18.4 de la Constitución Española de 1978: "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". Este artículo remite al desarrollo legislativo la "limitación del uso de la informática"[63], cumplido con la publicación de la LORTAD.

Sin embargo, el desarrollo del proyecto europeo y la publicación tanto del Convenio 108 como de la DPD, hacen necesaria la actualización de las normas, que se cumplió con la

[62] NAVAS NAVARRO, S., "Computación en la nube..." cit. pág. 26. El dictamen del grupo de trabajo es el 8/2010, de 16 de diciembre de 2010, sobre derecho aplicable, donde estudia diversos casos en los que considerar o no los equipos localizados en territorio de la UE.

[63] REBOLLO DELGADO, L., *Biomedicina y protección….* cit. 146. La LORTAD nace con vocación de "hacer frente a los riesgos que para los derechos de la personalidad puede suponer el acopio y tratamiento de datos por medios informáticos". Esta ley configura la Agencia de Protección de Datos (ADP) como un ente de Derecho Público (cuyas funciones, estructura orgánica y demás disposiciones se establecieron en el Real Decreto 428/1993, por el que se aprueba el Estatuto de la Agencia de Protección de Datos. La Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, cambió la denominación de la Agencia por la actual AEDP (añadiendo el "española") modificando la LOPD.

aprobación de la LOPD en 1999, con un contenido que abarca (con la protección que le confiere el mandato constitucional a la regulación del contenido del derecho fundamental a la protección de datos[64]) las disposiciones generales que enmarcan el objeto de la ley y su ámbito de aplicación, los principios del tratamiento, que incluye la regulación del consentimiento, el régimen de los datos sensibles y la comunicación de datos, los derechos de las personas y el movimiento internacional de datos[65]. El desarrollo se produce por el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (en adelante, RLOPD). Llama la atención en primer lugar la diferencia entre la aprobación de la ley, en 1999 y de su reglamento de desarrollo 8 años más tarde. Y, por encima de todo ello, el hecho de que, en un contexto de cambios rápidos y radicales, una normativa esté en vigor sin apenas cambios desde 1999[66].

En la actualidad, por la influencia del RGPD, el Consejo de Ministros aprobó el Proyecto de Ley Orgánica de Protección de datos de Carácter Personal con fecha de 10 de noviembre de 2017, que adapta la normativa de protección de datos a las exigencias del nuevo reglamento europeo.

La autoridad española encargada de la protección de datos es la Agencia Española de Protección de Datos (AEDP), creada por la LORTAD en su título VI y definida de igual modo en el art. 79 de la LOPD. La agencia tiene potestad normativa (Instrucciones y Recomendaciones), perteneciendo también al GT 29, potestad sancionadora administrativa, y es el órgano encargado de velar por el cumplimiento de la legislación sobre protección de datos.

[64] SERRANO PEREZ, M.M., *El Derecho Fundamental a la Protección de Datos. Derecho Español y Comparado*, Thomson, Madrid, 2003, pág. 98.

[65] La LOPD pertenece a la tercera generación de legislaciones europeas de protección de datos. La primera generación, incluye leyes más sencillas (porque el escaso desarrollo de la informática aún no supone un riesgo evidente para los datos personales) y exigen autorización previa para la creación y funcionamiento de bancos de datos a través de órganos específicos (Alemania en 1977, pero también se pueden incluir la ley austriaca de 1978, o la regulación de Luxemburgo de 1979). Las leyes de segunda generación incluyen el concepto y la especial protección de los datos sensibles (Ley francesa de 1978, La *Privacy Act* de Gran Bretaña de 1984 y la *Privacy Act* de Irlanda de 1988). La tercera generación se orienta hacia la protección del individuo frente a la acumulación de datos personales, incluyendo los datos sensibles en su regulación y considerando los datos no como meros transmisores de información, sino como datos con funcionalidad. En SERRANO PEREZ, M.M., *op. cit.* págs. 99-103.

[66] Quedando una legislación anacrónica y falta de actualización. Esta opinión es compartida por la mayoría de autores: GIL GONZÁLEZ, E., *Big data y datos personales*…cit. pág. 7, HERRÁN ORTIZ, A., *op. cit.* 637.

3.1.4.- Derechos ARCO.

Son de especial relevancia en la regulación sobre protección las facultades concretas que la normativa otorga a las personas para realizar el control sobre sus datos, que pueden aglutinarse en los llamados derechos ARCO: derechos de acceso, rectificación, cancelación y oposición. En palabras del Tribunal Constitucional, en sentencia 292/2000, de 10 de noviembre, estos derechos suponen "el reconocimiento del derecho a ser informado de quien posee sus datos personales y con qué fin, y el derecho a oponerse a esa posesión o uso requiriendo a quien corresponda que ponga fin las acciones que esté efectuando"[67].

La regulación específica de estos derechos la encontramos en todos los cuerpos normativos que regulan la materia:

- RGPD: recogidos en el capítulo III (Derechos del interesado), en los artículos 15 a 17 (acceso, rectificación y supresión/cancelación) y 21 (oposición). El RGPD añade nuevos derechos del interesado a los derechos ARCO, que se pueden resumir en: configuración del derecho al olvido (art. 17); derecho a la limitación-restricción del tratamiento en determinadas circunstancias (art. 18); derecho a la portabilidad de datos (art. 20)[68]; derecho a ser informado de cualquier brecha de seguridad (art. 34); y el derecho a ser indemnizado de los daños y perjuicios materiales o inmateriales sufridos como consecuencia de una infracción del Reglamento (art. 82)[69].

- LOPD: aunque la regulación básica y su procedimiento se encuentra en los artículos 15,16 y 17, es en el RD 1720/2007, que desarrolla la Ley Orgánica especialmente en los derechos ARCO, que dedica su Título III al desarrollo de los derechos (arts. 20-36).

[67] Es decir, "exigiendo al titular del derecho que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o cancele". Fundamento jurídico 7, glosado en REBOLLO DELGADO, L., SERRANO PÉREZ, M.M., *Manual de Protección de Datos,* Dykinson, Madrid, 2014, pág. 173.

[68] Aunque este, más que ser un nuevo derecho, podría configurarse como una especificación del derecho de acceso: permite al interesado obtener "en un formato electrónico estructurado y comúnmente utilizado" una copia de los datos que están siendo objeto de tratamiento, que debe permitir que esos datos puedan seguir siendo usados (se entiende que en otro sistema o aplicación). En MIRALLES, R., "El derecho a la portabilidad de los datos personales o prestaciones "premium" del tradicional derecho de acceso", en VALERO TORRIJOS, J. (Coord.), *La Protección de los Datos …,* cit. pág. 277.

[69] GARCÍA PÉREZ, R.M., *op. cit.* pág. 232-235.

Estos derechos son personalísimos, como se definen en el art. 23 del RLOPD, por lo que serán ejercitados por el interesado o afectado[70]. Las facultades que estos derechos otorgan pueden resumirse en lo siguiente:

- Derecho de acceso: el interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, su origen, así como de las comunicaciones realizadas o futuras. Hay que indicar que éste (como el resto), no es un derecho absoluto, por lo que tendrá restricciones respecto a determinadas informaciones incluidas en determinados ficheros[71]. También tiene una restricción temporal, en cuanto el art. 15.3 LOPD establece que este acceso no puede ser ejercitado a intervalos inferiores a 12 meses, mientras que el RGPD no limita el tiempo que ha de transcurrir.

- Derechos de rectificación y cancelación: el primero consiste en la posibilidad del interesado de hacer cumplir al responsable el principio de calidad de los datos, cuándo estos sean erróneos o incompletos. Supone un control "*a posteriori"* (como los derechos de cancelación y rectificación), en cuanto permiten a su titular ejercer control sobre datos que ya han sido recabados y registrados con anterioridad[72].Aunque no son lo mismo, se regula de forma conjunta el Derecho de cancelación: implica el bloqueo de los datos, mediante la identificación y reserva de los mismos para impedir su tratamiento (aunque se exceptúa el uso por las Administraciones Públicas (en adelante AAPP), Jueces y Tribunales en determinadas circunstancias). La regulación se hace de forma conjunta ya que tienen una causalidad común: si los datos son erróneos, incompletos, excesivos o se recogieron mediante procedimientos desleales o engañosos, o sin consentimiento del afectado, podrán ser rectificados o cancelados[73]. El derecho de cancelación, reconocido por la normativa de protección de datos, es el que ha dado pie, entre otros derechos, al llamado "derecho al olvido" especialmente relevante en la actualidad y en el mundo de Internet[74].

- Derecho de oposición: derecho que se puede referir o bien a que el interesado se oponga al tratamiento de todos los datos o solo de alguno de ellos. Este supone un

[70] BUREAU VERITAS FORMACIÓN, *Ley de protección de datos personales. Manual práctico para la protección de los datos personales de las personas físicas,* FC Editorial, Madrid, 2009, pág. 115.

[71] SERRANO PEREZ, M.M., *op. cit.*, pág. 344. Aunque no se determinan qué tipo de ficheros, si indica que se podrán denegar el derecho de acceso a determinados ficheros si el responsable encuentra una justificación constitucional para ello y habilitación legal expresa. El RLOPD permite la denegación de este derecho en dos supuestos (art. 30): cuando se ejercita sin respetar el plazo de doce meses de espera desde la última solicitud (art. 30.1 RLOPD) o bien cuando así lo prevea una Ley o una norma de derecho comunitario que impida al responsable revelar a los afectados el tratamiento de los datos. REBOLLO DELGADO, L., SERRANO PÉREZ, M.M., *Manual de Protección…,* cit. 191.

[72] GARRIGA DOMÍNGUEZ, *op. cit*. pág. 209.

[73] GARRIGA DOMÍNGUEZ, *op. cit*. pág. 211.

[74] Muy interesante al respecto SIMÓN CASTELLANO, P., *op. cit.* 2012.

derecho que busca la protección "*a priori*", porque pretende evitar que se recojan datos de determinada persona. Para que nazca este derecho es necesario que la recogida de los datos no haya precisado del consentimiento del afectado y que éste tenga motivos fundados y legítimos relativos a una concreta situación personal[75].

3.2.- El marco tecnológico y su normativa en relación con la protección de datos.

El contexto tecnológico, en el que la protección de datos se ve especialmente vulnerable, hace que sea necesario incluir en el punto de vista legislativo las nociones de la regulación general que protege al usuario que interactúa en internet (ya sea como consumidor o usuario, de servicios online o productos), también de las normas que protegen de la vulneración a los usuarios a través de la competencia desleal entre empresas, y de las diferentes normativas en las que se incluyen menciones a la protección de datos.

3.2.1.- Normativa de Consumidores.

Al hablar de la presencia de personas en internet, indudablemente ha de venir a la cabeza el Derecho de Consumidores, que protege a consumidores y usuarios en los distintos ámbitos en los que éstos se enfrentan con el mundo empresarial. Se ha de tener en cuenta que, en relación con consumidores e internet, se estará hablando de la protección de estos en cuanto a la contratación a distancia.

En primer lugar, y tratándose de contratación a distancia, tenemos la Directiva de 25 de octubre de 2011, sobre los Derechos de los Consumidores[76] en el que, entre otras cosas, regula los contratos celebrados a distancia y los contratos celebrados fuera de los establecimientos mercantiles. Esta normativa ofrece al consumidor los deberes de información precontractual, los requisitos formales de la contratación y, ante todo, la ampliación del derecho a desistir[77].

En la normativa española, la protección de consumidores se basa en el Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes

[75] VEGA VEGA, J.A., *op. cit.* pág. 379.

[76] Directiva 2011/83/UE del Parlamento Europeo y del Consejo, de 25 de octubre de 2011, sobre los Derechos de los Consumidores, por la que se modifican la Directiva 93/13/CEE del Consejo y la Directiva 1999/44/CE del Parlamento Europeo y del Consejo y se derogan la Directiva 85/577/CEE del Consejo y la Directiva 97/7/CE del Parlamento y del Consejo.

[77] ARROYO AMAYUELAS, E., "La contratación a distancia en la Directiva de protección de los derechos de los consumidores" en CÁMARA LAPUENTE, S. (Dir.), ARROYO AMAYUELAS, E. (Coord.), *La revisión de las normas europeas y nacionales de protección de los consumidores. Más allá de la Directiva sobre Derechos de los consumidores y del Instrumento opcional sobre un Derecho Europeo de la compraventa de octubre de 2011*, Civitas, Navarra, 2012, pág. 246-247. Actualmente se encuentra en tramitación la Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a determinados aspectos de los contratos de compraventa en línea y otras ventas a distancia de bienes (COM/2015/0635)

complementarias (TR-LGDCU), que precisamente fue modificado en 2011 por la publicación de la Directiva 2011 sobre contratos celebrados a distancia, por la Ley 3/2014, de 27 de marzo, por la que se modifica el texto refundido del TR-LGDCU.

3.2.2.- Prácticas desleales.

La regulación sobre las prácticas desleales se concreta en la Unión Europea en la Directiva, de 11 de Mayo de 2005, relativa a las prácticas comerciales desleales[78]. Las prácticas desleales afectan al consumidor en cuanto su consecuencia última es la merma importante de la libertad de elección o decisión de los consumidores afectados, ya que este tipo de prácticas pretende mover a los usuarios a tomar decisiones que de otro modo no habrían adoptado (ésta es la exigencia del artículo 8 de la Directiva sobre las prácticas comerciales desleales)[79].

Así, el envío de publicidad no deseada a los servicios de correo electrónico (*Spam)* se concreta en los apartados 25 y 26 del Anexo I (donde se explicita qué tipo de prácticas se consideran desleales) como una forma de acoso que, mediante la persecución, el incómodo o el apremio al consumidor, pretenden obtener una decisión de compra o determinar su comportamiento en el marco de la relación previamente establecida[80]. Por ello resulta imprescindible la protección de datos, en cuanto puede prevenir el uso del correo electrónico sin consentimiento para el envío de correos cuando el usuario no lo ha solicitado expresamente.

La normativa española que regula las prácticas desleales se encuentra en la Ley 3/1991, de 10 de enero, de competencia desleal (a partir de ahora Ley de competencia desleal), que fue modificada por la Ley 29/2009, de 30 de diciembre por la que se modifica el régimen legal de la competencia desleal y de la publicidad para la mejora de la protección de los consumidores y usuarios, para adaptarla a la normativa europea más reciente.

3.2.3.- Propuesta de Directiva de Contenidos Digitales.

Aunque no de forma directa, la Propuesta de Directiva de 9.12.2015, sobre determinados aspectos de los contratos de suministro de contenidos digitales, afecta a ciertos servicios que, aunque no se tratarán de forma directa, se pueden englobar en las actividades que hacen uso de nuestros datos. Hablamos de servicios de C*loud Computing* o bien de

[78] Directiva 2005/29/CE del Parlamento Europeo y del Consejo, de 11 de Mayo de 2005, relativa a las prácticas comerciales desleales de las empresas en sus relaciones con los consumidores en el mercado interior

[79] MASSAGUER FUENTES, J., "Prácticas comerciales agresivas", FERNANDEZ LÓPEZ, *op. cit.* pág. 85.

[80] MASSAGUER FUENTES, J., *op. cit.* 82.

suministro de contenidos en formato digital como por ejemplo vídeo, audio, aplicaciones o juegos digitales (plataformas como *Netflix* o bien la *Play Store* son suministradores de servicios totalmente digitales). La especial relevancia de esta fuente normativa reside, por un lado, en la consideración de servicios a los que aplicar esta normativa aquellos contratos de suministro "gratuitos", es decir, aquellos que no cobran un precio en dinero, sino que lo hacen, generalmente, a cambio de datos[81]. De otro lado, la nueva consideración que la propuesta realiza sobre la conformidad.

3.2.4.- Otra normativa con referencias a la protección de datos.

Al margen de la normativa principal sobre protección de datos, existen normas sectoriales (especialmente relacionada con los servicios de comunicaciones electrónicas), que regulan la materia:

- La Ley 34/2002, LSSICE, en la que, además de establecer en su capítulo II un régimen de publicidad y transparencia de los prestadores de servicios, regula la obligación de retención de datos de conexión y tráfico (art. 12)[82]. También prohíbe el envío de *spam* (vid. Apartado 5.3.2). La relación entre la LOPD y la LSSICE queda clara en esta última, en cuanto indica en su art. 19: "En todo caso, será de aplicación la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y su normativa de desarrollo, en especial en lo que se refiere a la obtención de datos personales, la información de los interesados y la creación y mantenimiento de ficheros de datos personales"[83]
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones (en adelante, LGT), que dedica su capítulo III del Título III a las obligaciones de protección de datos[84].

[81] "Sin duda, las instituciones comunitarias han tomado en serio el ingente valor económico y de cambio que tiene la información (datos)" CÁMARA LAPUENTE, S., "El régimen de la falta de conformidad en el contrato de suministro de contenidos digitales según la Propuesta de Directiva de 9.12.2015", *Indret (Revista para el análisis del Derecho),* Barcelona, 2016, pág. 21.

[82] Estos datos han de ser guardados durante un periodo máximo de 12 meses, reduciéndose el periodo de retención de los datos, y legitimando la recogida de los mismos solo a los imprescindibles para identificar el origen de los datos y el momento en el que se inició la prestación del servicio (la motivación de esta retención tienen que ver con su uso en investigaciones criminales o la salvaguarda de seguridad pública[82], especialmente relevante actualmente).

[83] PANIZA FULLANA, A., "Tratamientos para actividades de publicidad y prospección comercial" en MARTÍNEZ MARTÍNEZ, R., *Protección de datos. Comentarios al Reglamento de desarrollo de la LOPD,* Tirant lo Blanch, Valencia, 2009, pág. 254.

[84] Establece para los operadores que exploten redes públicas de comunicaciones o que presten servicios de comunicaciones electrónicas disponibles al público la obligación de garantizar en el ejercicio de su actividad la protección de datos de carácter personal conforme a la legislación vigente (art. 41) y un elenco de derechos relacionados con la protección de datos (art. 48)

4.- La obtención del consentimiento.

Aunque el consentimiento se configura en la materia de protección de datos como uno de los pilares fundamentales, muchas son las voces que indican que éste es insuficiente. Las numerosas excepciones y los nuevos retos que presenta la prestación del consentimiento en Internet dejan este requisito de la prestación del consentimiento como uno de los supuestos, entre varios, que legitima el tratamiento de los datos[85].
En este apartado veremos cuál ha sido la regulación sobre el consentimiento hasta ahora, de qué problemas puede adolecer, y en qué mejora (o no) el consentimiento el RGDP, además de los nuevos mecanismos de protección de datos. Por último, veremos la difusa línea que se crea al recabar el consentimiento para contratar y para el tratamiento de datos y si se puede hacer de forma conjunta (en las cláusulas de los famosos "términos y condiciones" de los contratos).

4.1.- Regulación actual.

El art. 7 de la DPD y el art. 6 de la LOPD (en el apartado uno la regla general, en el dos, otros casos en los que el consentimiento no es necesario) regulan de forma muy similar los fundamentos jurídicos que permiten a las empresas tratar los datos personales. Estos artículos establecen que el tratamiento de datos se puede realizar siempre que se cumpla alguna de las siguientes condiciones:

a) Contar con el consentimiento inequívoco del interesado;
b) Que el tratamiento sea necesario para ejecutar un contrato en el que el interesado sea parte;
c) Que el tratamiento sea necesario para proteger un interés vital del interesado;
d) Que el tratamiento sea necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público;
e) Que el tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero a quien se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado.

Como se puede ver en esta enumeración, aunque el consentimiento es el primero de los supuestos que legitiman para el tratamiento de datos, no es el único y se establecen un buen número de opciones para no recabarlo (entendidas en la legislación española como

[85] ANDREU MARTINEZ, M.B., PLANA ARNALDOS, M.C, "El poder de disposición del titular como facultad principal del derecho a la protección de los datos personales: su efectividad en el actual escenario tecnológico" en VALERO TORRIJOS, J. (Coord.), *La Protección de los Datos …,* cit. pág.131; REBOLLO DELGADO, L., SERRANO PÉREZ, M.M., *Manual de Protección…,* cit. 111; OLIVER-LALANA, D., MUÑOZ SORO, J.F., "El mito del consentimiento y el fracaso del modelo individualista de protección de datos", en VALERO TORRIJOS, J. (Coord.), *La Protección de los Datos …,* cit. pág. 154-156.

excepciones). Sin embargo, no hemos de dejar de lado la importancia evidente del consentimiento, pero sí evidenciar que su relevancia práctica no se corresponde con la importancia teórica que pretende. En este punto, es importante establecer qué entendemos por consentimiento y las características que éste ha de tener para considerarse válido. Actualmente existen dos sistemas para manifestar el consentimiento en el ámbito tecnológico: el sistema *opt-in* y el *opt-out*. Mientras que el primero exige que el usuario manifieste un consentimiento expreso y positivo anterior a recabar los datos (rellenando, por ejemplo, la casilla creada a tal efecto), el segundo implica que el individuo debe manifestar su oposición en un periodo determinado, desde que es informado de que se recabarán sus datos (bien rellenando una casilla diferente o manifestándolo a la organización por el medio oportuno)[86]. La regulación española opta por el sistema *opt-in* cuando supedita a la solicitud por parte del usuario o su consentimiento para el envío de comunicaciones comerciales (*Spam*) en el art. 21 LSSICE[87], optando por el sistema *opt-out* para el tratamiento de datos general, como se verá más adelante.

La DPD y la LOPD definen el consentimiento de forma similar (en la primera en el art. 2.h; en la segunda, el art. 3.h.) estableciendo que es una manifestación de voluntad mediante la cual el interesado consienta el tratamiento de datos personales que le conciernen. Sin embargo, ambas incluyen ciertas características de este consentimiento que son esenciales para entender la protección que este mecanismo proporciona: el consentimiento ha de ser libre, informado, específico e inequívoco.

El consentimiento ha de ser *libre*, lo cual hace referencia a alguno de los vicios que afectan a la voluntad según el Código civil[88]. El consentimiento únicamente puede ser válido si el interesado tiene una opción real de elegir si lo da o no y, además, si no hay ningún riesgo de engaño, intimidación o consecuencias negativas significativas en caso de que no consienta.

La segunda característica del consentimiento se basa en la *información*. Ello implica que, en el momento de solicitarse el consentimiento, debe suministrarse toda la información necesaria, de forma clara y comprensible. Las cuestiones sobre qué hay que informar se encuentran reguladas en el art. 10 de la DPD y en el art. 5 de la LOPD (Identidad del responsable; fines del tratamiento de datos; destinatarios o categorías de destinatarios, carácter obligatorio o no de la respuesta, existencia de derechos ARCO). Esta condición resulta imprescindible para un consentimiento válido, ya que el interesado ha de poder conocer las consecuencias que se derivarán de darlo[89]. Esta necesidad de información se

[86] GIL GONZÁLEZ, E., *Big Data, privacidad…,* cit. Pág. 79.
[87] PANIZA FULLANA, A., "Tratamientos para actividades…", cit. 255.
[88] REBOLLO DELGADO, L., SERRANO PÉREZ, M.M., *Manual de Protección…,* cit. 114.
[89] Este deber de información es especialmente relevante en caso de menores de edad, sobre todo por el hecho de que, desconociendo los riesgos que puede tener prestar sus datos por ver los contenidos de una

torna especialmente relevante cuando existe la posibilidad de transmitir esos datos a terceros países, puesto que el interesado debe saber que sus datos se transmiten a un país que carece de la protección adecuada[90].

Para ser válido, el consentimiento para el tratamiento de datos ha de ser *específico*. El Dictamen 15/2011, del GT 29 indica que no es válido si se recaba el consentimiento para el tratamiento de datos indiscriminado: el interesado ha de saber el contexto limitado de qué datos se tratarán y los motivos del tratamiento (está claramente relacionado con el consentimiento informado). Sin embargo, el GT 29 puntualiza que tampoco será válida una cláusula que abarque "todos los fines legítimos". Por ello, se extrae que el consentimiento podría tener que recabarse más de una vez si la finalidad cambia (por ejemplo, si se recabó información para el envío de información de nuevos productos y promociones, pero, posteriormente, se quieren ceder los datos a terceros, ello requeriría un nuevo consentimiento[91]).

Por último, el consentimiento ha de ser *inequívoco*. Este es el requisito más complejo y discutido. Se establece en el art. 7.a de la DPD, y ello significa, según el GT 29 que "el procedimiento de su obtención y otorgamiento no tiene que dejar *ninguna duda* sobre la intención del interesado de dar su consentimiento". Ello significa, además, que el responsable del tratamiento debe asegurarse de que la persona que da su consentimiento es efectivamente el interesado. En la legislación española, el término "inequívoco" aparece en el art. 5 (respecto a la información) y en el art. 6 (respecto al consentimiento) LOPD.

Pero ¿significa ello que el consentimiento ha de ser *expreso*? En la legislación española queda claro que no, ya que el consentimiento expreso se regula tan solo para los tratamientos de datos relativos a la ideología, religión, creencias y afiliación sindical (art. 7.2 LOPD) o a datos sobre la salud, el origen racial y la vida sexual (art. 7.3 LOPD), no siendo así obligatorio para ninguna otra categoría de datos. En el caso de la normativa europea, el GT 29 especifica en su Dictamen 15/2011, que esta característica puede conseguirse o bien mediante "un claro consentimiento expreso o bien basarse en determinados tipos de procedimientos para que las personas manifiesten un claro consentimiento deducible". Ello nos deja con la duda: ¿es válido, entonces, el silencio? De nuevo la legislación española no deja dudas[92]: el art. 14.2 RLOPD establece que el

página (finalidad), pueden proporcionar una edad falsa (bien porque piensan que sus padres no se lo permitirían o bien porque la edad real puede hacer que se les deniegue el acceso a la página). En GARRIGA DOMÍNGUEZ, *op. cit.* 189.

[90] GIL GONZÁLEZ, E., *Big Data, privacidad…,* cit. Pág. 68.

[91] Dictamen 15/2011, sobre la definición de consentimiento, adoptado el 13 de junio de 2011, del Grupo de Protección de datos del art. 29 (En adelante Dictamen 15/2011).

[92] ANDREU MARTINEZ, M.B., PLANA ARNALDOS, M.C., *op. cit.* pág. 140.

responsable podrá dirigirse al afectado y después de informarle de los términos sobre el tratamiento darle "un plazo de treinta días para manifestar su negativa al tratamiento, advirtiéndole de que en caso de no pronunciarse a tal efecto se entenderá que consiente el tratamiento de sus datos de carácter personal". En su Dictamen 15/2011 el GT 29 expresa, en una serie de ejemplos, la posibilidad de que el silencio no suponga una situación inequívoca (la falta de respuesta a un correo electrónico no significa que la persona de su consentimiento válido e inequívoco), pero cierra el apartado "animando" a que los responsables usen procedimientos y mecanismos que no dejen duda[93]. Además, en las conclusiones indica que las casillas preseleccionadas o el uso de parámetros por defecto del navegador para recopilar datos, plantean serios problemas de consentimiento inequívoco, por lo que no queda tan claro como en la legislación española.

Por último, relativo al consentimiento, queda determinar la revocación del mismo. En la LOPD esta opción se establece en el art. 6.3, en la que indica que se permite la revocación "cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos", aunque no queda claro qué significa que implica "causa justificada" (concepto indeterminado)[94]. En la normativa europea no indica nada de la revocación, sin embargo, la existencia de los derechos ARCO, entre los cuales existe el derecho de oponerse y cancelar los datos, da pie a un posterior cambio de opinión (siempre por motivos fundados) que permita no recabar más los datos del interesado.

4.2.- Reglamento UE.

Si nos preguntamos cuál será la regulación respecto al consentimiento de la normativa que entrará en vigor el 25 de mayo de este año, nos encontramos que el consentimiento y alguna de sus condiciones ha sido el aspecto más controvertido en el proceso normativo. El art. 6 del RGPD sigue estableciendo como una de las posibilidades (de nuevo la primera entre varias) el consentimiento, como mecanismo legitimador del tratamiento de datos personales. Ello no difiere mucho de lo visto en la normativa anterior. El artículo 4.11 RGPD define el tratamiento como "toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen". En esta definición podemos encontrar los aspectos diferenciadores respecto a la normativa aún en vigor: aunque se mantienen iguales las condiciones de información, especificidad

[93] Dictamen 15/2011, sobre la definición de consentimiento, págs. 27-28.

[94] Hay que aclarar que esta opción de revocación no es absoluta, existiendo dos restricciones: una, que exista una causa justificada (que debería entenderse, ante la indeterminación de la definición como cualquier motivo legal y razonable) y que no provoque efectos retroactivos, es decir, que la revocación no ha de tener efectos antes de que la misma se produzca. En DELGADO, L., SERRANO PÉREZ, M.M., *Manual de Protección…,* cit. 127.

y libertad (aunque el resto del texto del RGPD imponga distintos matices), existe un gran matiz respecto a la manifestación inequívoca.

Empezando por el consentimiento libre, el art. 7.2 del RGPD indica que, si el contexto de la declaración de consentimiento se da de forma escrita, ésta deberá presentarse de tal forma que se distinga del resto de asuntos (con lenguaje claro y sencillo y de fácil acceso, no, por ejemplo, en letra muy pequeña al reverso), existiendo falta de libertad cuando no se permita dar el consentimiento por separado a las distintas operaciones del tratamiento[95]. A ello se une lo considerado en el art. 7.4 que indica que, para la evaluación de que el consentimiento ha sido dado libremente, se tendrá en cuenta si la ejecución del contrato se supedita al consentimiento del tratamiento de datos personales[96].

En cuanto a las características del consentimiento específico e informado, el RGPD no contiene grandes novedades. De nuevo, los fines del tratamiento de datos han de ser concretos y explicitados al interesado (en el caso del consentimiento específico). En cuanto de la información, el reglamento se esfuerza en ampliar la transparencia, ya que la complejidad de las prácticas de recolección de datos (en especial en internet) hacen difícil que la persona pueda ser consciente y controlar la información que comparte. Por ello el art. 12 indica que la información debe facilitarse de forma "concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo"[97].

El mayor cambio se pretendió en el consentimiento inequívoco. A diferencia de la DPD, que permite que el consentimiento fuera revelado ya fuera por escrito, verbalmente o bien por un comportamiento del que pudiera razonablemente deducirse dicho consentimiento[98], el RGPD se decanta por exigir en este aspecto una declaración o una clara acción afirmativa (art. 4.11). Se acerca así a lo que las distintas voces (GT 29 y distintos organismos como la AEPD, que seguía el criterio del Dictamen 15/2011) pedían para la "aclaración" del término inequívoco. Sin embargo, como he indicado, fue mayor el cambio que se pretendió al que realmente se llevó a cabo por el legislador en el RGPD:

[95] Expresado en el considerando 43 del RGPD. En GARCÍA PÉREZ, R.M., *op. cit.* pág. 223.

[96] Referido a la libertad del consentimiento y este último apartado del art. 7 es interesante saber que el considerando 42 del RGPD se remite a la normativa de consumidores, en especial en lo tocante a los contratos de adhesión (aquellos que están predispuestos por el empresario en los que claramente existe un desequilibrio, en los que el interesado no puede negociar, como son la mayoría de los que se encuentran en las aplicaciones y en las páginas web, en los que basta marcar una casilla de "acepto y he leído" las condiciones), para evitar las cláusulas abusivas que pudieran contener, incluso referidas al consentimiento. En GARCÍA PÉREZ, R.M., *op. cit.* pág. 224.

[97] GARCÍA PÉREZ, R.M., *op. cit.* pág. 223 y ANDREU MARTINEZ, M.B., PLANA ARNALDOS, M.C., *op. cit.* pág. 135, referido a la propuesta de reglamento. Así, se recoge las recomendaciones realizadas por el GT 29 en el Dictamen 15/2011.

[98] ANDREU MARTINEZ, M.B., PLANA ARNALDOS, M.C., *op. cit.* pág. 139.

el devenir normativo[99], desde la propuesta de Reglamento de 2012 hasta el RGPD de 2016, sufrió grandes cambios y fue uno de los aspectos más controvertidos de la tramitación normativa. En las primeras redacciones[100] tanto en los considerandos iniciales que trataban el consentimiento (considerando 25 en ambos) como en la definición del art. 4 se indicaba que el consentimiento, además de libre, específico e informado, debía ser explícito (mediante declaración o mediante acción afirmativa)[101]. Además de ello, indicaba que el silencio o la inacción de ningún modo constituirían consentimiento.

Finalmente, este incremento tan notable de la protección de datos mediante el control del usuario sobre su consentimiento, que hubiera supuesto exigir el consentimiento explícito y la no aceptación del silencio o la inacción no se ha producido. Sin embargo, el considerando 32 RGPD sí que ha incluido la parte que pretende evitar el silencio como consentimiento: "Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento", y la definición del consentimiento reduce las posibilidades de consentimiento a una declaración o una clara acción afirmativa, por lo que se incrementa (aunque quizá no suficiente) el posible control del interesado.

En cuanto a lo que se ha llamado en Derecho español la revocación del consentimiento, el RGPD lo incluye en su art. 7 (Condiciones para el consentimiento), apartado 3, de forma que el interesado podrá "retirar su consentimiento en cualquier momento" también con la imposibilidad de causar efectos retroactivos. Respecto a la normativa anterior, no se condiciona la retirada del consentimiento (como sí lo hacía el art. art. 6.3 LOPD) y se especifica que "será tan fácil retirar el consentimiento como darlo", lo cual sí supone más derechos para el interesado.

[99] Así, el informe de la Presidencia presentado al Consejo de la UE, sobre la Propuesta de Reglamento indicaba que "la mayoría de los Estados miembros concuerda en que no era realista el requisito del consentimiento <<expreso>> en todos los casos", y se sugiere volver al término inequívoco. ANDREU MARTINEZ, M.B., PLANA ARNALDOS, M.C., *op. cit.* pág. 141. También se pone en relieve que mayor atención por el consentimiento expreso, sin tener en cuenta el valor o los usos de los datos, podría ralentizar la innovación y los avances sociales, en GIL GONZÁLEZ, E., *Big Data, privacidad…,* cit. pág. 81.

[100] Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos de 25 de enero de 2012 COM (2012), y la Resolución legislativa del Parlamento Europeo, de 12 de marzo de 2014, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos COM (2012).

[101] GARCÍA PÉREZ, R.M., *op. cit.* pág. 227-228 presenta los cuadros comparativos entre las propuestas y resoluciones, y el texto final del reglamento, de todos los apartados del cuerpo normativo donde el consentimiento es nombrado o definido, donde se puede ver claramente los cambios que el texto ha ido sufriendo hasta su definitiva aprobación.

4.3.- Más allá del consentimiento: otros mecanismos de protección.

Sin embargo, a todo lo anterior hay que sumar que el consentimiento no es considerado, en contextos tecnológicos, el mejor sistema para proteger los datos del interesado: la mayoría de las personas no lee las políticas de privacidad o, si lo hacen, no las comprenden[102] (aunque las páginas no dejen avanzar sin "leerlo"). Ello hace que, a pesar de la preocupación del legislador por reforzar el consentimiento, éste haya quedado un tanto obsoleto por la forma de prestarlo (basado en la lectura de esa información que se presenta en las páginas) en los contextos tecnológicos.

Ante estos problemas que surgen del consentimiento, hay distintos mecanismos que se pueden adoptar, más cercanos a la prevención ante los quebrantamientos del uso de los datos personales por parte de las corporaciones, y un sistema más americano (en el que las empresas adquieran la responsabilidad sobre los datos personales que hayan recabado) que complementen la exigencia del consentimiento. El Reglamento ha venido a reforzar, de algún modo, la llamada privacidad por defecto y la privacidad desde el diseño: la necesidad, por parte del responsable del tratamiento, de adoptar medidas de carácter técnico u organizativo que minimicen el número de datos personales tratados y aseguren que, por defecto, sólo se trataran los datos personales imprescindibles y necesarios para cada objetivo, de forma que sea el usuario quien puede cambiar la configuración para permitir otras utilidades[103] (Regulado en el art. 25 del RGPD).

También aparece en el Reglamento la posibilidad de realizar evaluaciones de impacto, es decir, un análisis del tratamiento que se realizará, de forma que se pueda saber (antes de implementar el tratamiento) si provocará o no daños a los derechos y libertades de los interesados. Esta evaluación de impacto se regula en el art. 35 del RGPD y es obligatoria en ciertos casos (apartado 3) muy relacionados con el tratamiento de los datos por las

[102] En encuestas realizadas por la Agencia Vasca de Protección de Datos y el Observatorio Aragonés de la Sociedad de la Información (OASI), se evidencia esta realidad: en las encuestas del OASI en 2009, un 43% indicaron que leían con cuidado las cláusulas informativas; en las de la Agencia vasca, un 34% indicaron que siempre las leen, un 34% lo hacen alguna vez y un 31% nunca las leen. En OLIVER-LALANA, D., MUÑOZ SORO, J.F., *op. cit.* pág. 178-179. De la misma opinión es GIL GONZÁLEZ respecto a la inutilidad del consentimiento en contextos tecnológicos y cuando el *Big Data* entra en acción al tratar los datos, en GIL GONZÁLEZ, E., "*Big data* y datos personales…" cit. pág. 10. Actualmente, en el Informe de la Protección de datos personales de enero de 2017, publicado por el Gabinete de Prospección sociológica de la Agencia Vasca de Protección de Datos indica que ante la pregunta "¿Suele leer las políticas de privacidad de las páginas web que visita?" un 54% indica que nunca o casi nunca, un 28% indica que lo hace a veces y tan solo un 17% indica que lo hace siempre o casi siempre. Como se puede ver, la lectura de estas políticas que permiten un consentimiento informado no se realiza por parte de los usuarios, por mucho que estén a su disposición.

[103] GIL GONZÁLEZ, E., *Big Data, privacidad…,* cit. pág. 136.

nuevas tecnologías (evaluación sistemática y exhaustiva en tratamientos automatizados, tratamientos a gran escala o zonas públicas).

Especial mención, como mecanismo que se acerca a la autorregulación estadounidense, recae sobre el art. 24.1 del RGPD, en el que regula la responsabilidad de los responsables del tratamiento. Con ello, el RGPD pretende trasladar a las empresas la determinación de medidas que respondan de manera adecuada y eficaz a los riesgos de los tratamientos de datos[104].

4.4.- Finalidades lícitas del consentimiento: ¿para el contrato o, también, para recabar los datos?

En la práctica, cuando estamos navegando por Internet o nos damos de alta en determinadas *apps* o páginas web que requieren nuestros datos (para enviar información, contratar, u otros fines), rara vez nos encontramos con casillas separadas que permitan aceptar la política de protección de datos de un lado y, por otro lado, las condiciones y términos del contrato: damos un único consentimiento (generalmente en forma de *tick* en un cuadradito) para aceptar. Lo que no sabemos es que una de las cláusulas (o unas cuantas) suponen que aceptando el contrato estamos aceptando, también, el tratamiento de nuestros datos.

También es usual la siguiente situación: entramos en internet, para mirar determinado periódico y tenemos instalado un programa que permite bloquear anuncios (por ejemplo, *Adblock*) pero nos sale una ventana en la que indica que hay que desactivarlo para poder acceder a ese periódico (ofreciéndonos muy gentilmente ayuda para incorporar una excepción para la página de ese periódico). ¿Es esto lícito? ¿Para qué quieren esas páginas que yo vea los anuncios? ¿Funciona en este caso el consentimiento?

De forma previa, indicar que existen actualmente programas, como Adblock[105], que permiten bloquear estos anuncios o no permitir que las *cookies* presupongan nuestro consentimiento: son los bloqueadores de publicidad, pequeños programas que se instalan en nuestros navegadores de tal forma que se transmita a los programas de anuncios o a las *cookies* que el usuario no da su consentimiento a que los primeros se reproduzcan o

[104] GARCÍA PÉREZ, R.M., *op. cit.* pág. 242-243. 3

[105] Aunque pueda parecer novedoso, los bloqueadores de publicidad aparecen por primera vez en 2006, cuando el programa Ad Block Plus se lanzó en código abierto. En AGUADO, J.M., "La publicidad como problema. El impacto de los bloqueadores de anuncios en la industria del contenido digital", *Telos: Cuadernos de comunicación e innovación*, nº 103, 2016, pág. 6.

que las segundas se instalen en nuestro ordenador. Pero estos programas no siempre son permitidos por las páginas que se visitan.

Así, en el entorno digital se puede ver que muchas veces el acceso a productos o servicios (aparentemente desconectados del uso de datos personales, como puede ser un periódico), queda condicionado a la aceptación del tratamiento de los datos (o lo que es lo mismo, a la desconexión de los sistemas que lo bloquean) para finalidades distintas a las necesarias para acceder a la prestación solicitada[106]. Por ello, aunque se habla actualmente de consentimiento, en la práctica no se consiente: se asiente. Este cambio se debe a que, realmente, la acción de la persona se reduce a una mera aprobación para que una determinada actuación, que tendrá consecuencias jurídicas, pueda producirlas[107]. Hay que tener en cuenta que, en la mayoría de casos, no se trata de situaciones en las que el usuario da voluntariamente y por su propia iniciativa los datos, sino que se le pide que los dé al intentar realizar una acción (compra, suscripción a determinado servicio, entrada a una red social, etc.), es decir, no es espontánea, sino que responde a la iniciativa del operador[108].

El art. 7.2 RGPD soluciona esta cuestión indicando: "si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento". Por lo que queda claro que el clausurado contractual no puede ser utilizado por el predisponente de forma oculta para obtener el consentimiento para tratamientos de datos adicionales a los propiamente contractuales[109].

Hay que distinguir en este punto que la normativa de protección de datos (tanto la LOPD, la DPD como el RGPD) incluye como manera de legitimar el tratamiento de los datos que éstos sean recabados (sin necesidad por tanto de consentimiento) en el marco de una relación contractual, siempre que respondan a una finalidad determinada. Pongamos un

[106] GARCÍA PÉREZ, R.M., *op. cit.* pág. 205.

[107] Así lo defiende NAVAS NAVARRO, S., "Computación en la nube.." cit. pág. 30, en cuanto indica que esta aceptación lo es porque supone una declaración de voluntad unilateral cuya finalidad es legitimar la actuación del responsable (inmiscuyéndose así en la esfera privada del titular de los datos, los recoja y proceda a su tratamiento). También en el mismo sentido LLÁCER MATACÁS, cuando indica que la solicitud del empresario actúa como mecanismo de inducción de un negocio unilateral y cuyo contenido está predispuesto. *La autorización al… cit.* pág.126.

[108] LLÁCER MATACÁS, M.R., La *autorización al… cit.* pág. 128.

[109] Respecto a este tipo de contratos predispuestos, GARCÍA PÉREZ recuerda que es plenamente aplicable la normativa de consumidores: Directiva 93/13/CEE del Consejo, de 5 de abril de 1993, sobre cláusulas abusivas en los contratos celebrados con consumidores; el TR- LGDCU y la Ley 7/1998, de 13 de abril, sobre condiciones generales de la contratación. GARCÍA PÉREZ, R.M., *op. cit.* pág. 225.

ejemplo: si yo me suscribo a una revista, que además ofrece contenidos online, es imprescindible que esa empresa tenga datos que se refieran a mi dirección (para poder enviarme la revista), mi dirección de correo electrónico (para enviarme el contenido online, en caso de tener versión, o notificarme todos los cambios o novedades sobre mi suscripción) y mis datos de identificación y de pago (en caso de hacer un cargo domiciliado). No sería razonable pensar que esa empresa requiriera datos como mi posición geográfica (que pudiera recabarse si la revista tiene una app), o compras que realizo (mediante la instalación de *cookies* de la app o la página web).

¿Dónde surge el mayor problema? Hasta ahora, el uso de la tecnología permitía la anonimización[110] de estos datos: usados en bases de datos de dimensiones inimaginables, usaban por ejemplo todos los datos de geolocalización de los miles de usuarios de, por ejemplo, una red social, para análisis estadísticos. No había una identificación de las personas como tal. Sin embargo, el avance de la tecnología y sobre todo, de los modelos de mercado, llevan a un problema totalmente distinto: todos esos datos se usan en propio "beneficio" del usuario, creándose perfiles para enviarle información o publicidad personalizada y por tanto usando sus datos para señalarle de forma individualizada.

5.- Obtención y cesión de datos personales y publicidad.

Ya hemos visto que cualquier dato estará protegido si hace a la persona identificable y que, para recabarlos, será necesario (si no entra dentro del marco del resto de supuestos que legitiman a las empresas, vid. 4.1) el consentimiento del interesado. Sin embargo, todo ello no tendría ninguna relevancia sin que los usuarios generaran esos datos tan valiosos para las empresas: el cómo esos datos se incorporan a la red y cómo las empresas los recogen es el punto de partida sobre el que el Derecho ha de trabajar, para evitar las lagunas que permitan a las empresas recabar los datos sin el consentimiento del usuario. El uso de las tecnologías *Big data* permite transformar estos datos, recogidos bien del interesado o bien de terceros, de datos-materia prima a datos-conocimiento. Mientras los primeros son datos recogidos, generalmente mediante sistemas informáticos, sin tratar, manipular o cruzar con otros datos, de "bajo nivel"[111]. Los segundos son obtenidos a partir del tratamiento de los datos-materia prima por algoritmos matemáticos buscando determinadas finalidades, que generalmente se recogen en bases de datos[112].

[110] "La anonimización implica el tratamiento de datos de carácter personal de modo tal que no sea posible volver a identificarlos" en GIL GONZÁLEZ, E., *Big Data, privacidad…*, cit. pág. 84.

[111] Estos son definidos como *contenido digital online*, es un contenido desestructurado que proviene de diferentes fuentes y que comprende el más variado material (fotos, vídeos, comentarios u opiniones puestos en blogs, chats o bien redes sociales como *Twitter*) en NAVAS NAVARRO, S., "El internet de las cosas" en NAVAS NAVARRO, S., CAMACHO CLAVIJO, S., *Mercado Digital. Principios y reglas jurídicas*, Tirant lo Blanch, Valencia, 2016, pág. 40-42.

[112] Sin embargo, el uso de las nuevas tecnologías ha transformado las bases de datos que conocemos (estructuradas y claras) en conjuntos de datos masivos y confusos, que de por sí no dan información.

Y es que, aunque creamos que la información que compartimos en internet (a través de las redes sociales u otros medios) es la única que nosotros consentimos en dar a otros, ello no es verdad: muchos servicios aparentemente gratuitos de Internet (como pueden ser los correos electrónicos o los servicios de comunicaciones como *Whatssapp)* piden a cambio que el usuario permita el tratamiento y, sobre todo, la cesión de datos[113].
Hay que especificar, antes de entrar a concretar los problemas de la obtención y cesión de los datos que generamos y que las empresas tratan pueden ser de dos tipos: cuando los datos son obtenidos del propio interesado y cuando no son obtenidos del interesado. En el primer caso, el usuario suministra datos sobre su persona[114]. En el segundo, la empresa no obtiene los datos del interesado, comprendiendo tanto los casos en los que se obtienen de fuentes accesibles al público[115] como la cesión de datos, ésta última donde encontramos todo un mercado de datos

Hay que apuntar que la mera disposición de los datos por parte de los usuarios de internet no sería suficiente si no existieran empresas que se dedicaran a recabar esos datos y hacerlos útiles. Y surge una pregunta: ¿Para qué quieren las empresas esos datos? La respuesta no es sencilla. De forma general, usan toda la información para mejorar los productos y servicios que ofrecen, de forma que puedan ofertar lo más cercano a los gustos y preferencias de los consumidores.

Así, en este apartado veremos una de las formas más comunes en las que las empresas recogen datos de forma "consentida" por el usuario (las *cookies*), cómo usan esos datos (los perfiles) y también el régimen de la cesión de los datos a terceras empresas, como

Necesitan de procesos de "datificación" es decir, de conversión, para sacar información relevante. En NAVAS NAVARRO, S., "El internet de…", cit. pág. 45.

[113] GARRIGA DOMÍNGUEZ, *op. cit.* 42.

[114] Sobre este tipo de información es aplicable el régimen de consentimiento visto en el apartado 4. Sin embargo, hay que tener en cuenta que las empresas pueden no cumplir la normativa y recabar el consentimiento conjuntamente con la aceptación de términos y condiciones. Un ejemplo de ello es la app *Whatsapp Messenger*, que en su apartado de Información legal (accesible desde la app por el apartado Términos y Privacidad en Ayuda), indica que la aplicación tiene acceso a la totalidad de contactos de la agenda del usuario, datos de geolocalización, fotografías, datos de tráfico, etc. tanto para sí misma como para sus "proveedores externos", sin que para ello recabe, en el proceso de creación de la cuenta, el consentimiento para ello (ni se haya producido el aviso del cambio de las condiciones a los usuarios ya registrados). BLASI CASAGRAN, E., "La protección de datos en las aplicaciones de mensajería instantánea" en VALERO TORRIJOS, J. (Coord.), *La Protección de los Datos …,* cit. pág. 548-550. Comprobadas las políticas de la empresa a fecha 12/01/2017.

[115] Las fuentes accesibles al público son definidas en el art. 3.J LOPD (pero no en el RGPD), como "aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación" incluyendo la enumeración, de lista cerrada, de la fuentes consideradas como tal: los censos promocionales, los repertorios telefónicos y listas de personas pertenecientes a grupos profesionales (aunque con restricción de los datos que en éstas últimas pueden aparecer). Todas tienen una regulación específica y con bastante limitación de datos que pueden contener y los usos que pueden darse. En VILASAU SOLANA, M., *op. cit.* págs. 118-120.

forma de la recopilación de datos no obtenidos del propio usuario. Así, nos centraremos en la relación que puede existir entre la *publicidad comportamental* y los datos personales.

La publicidad comportamental, desde un punto de vista jurídico, se explica como aquella que busca conocer los hábitos de comportamiento y gustos del consumidor con el propósito de ofrecerle publicidad personalizada[116]. Y este es el punto de partida en el que los datos del consumidor se revalúan, sirviendo a las empresas.

5.1.- Obtención de los datos personales: el uso de *cookies*.

Si hace años, era necesario hablar con la persona en cuestión para saber de los gustos o preferencias de una persona, o bien seguirle durante un día de compras (con lo que ello podía suponer de coste tanto monetario como de tiempo), hoy en día la tecnología es capaz de monitorizar las preferencias o compras de un usuario mediante los clics que realiza en sus "paseos" por Internet, usando esos datos para enviar ofertas personalizadas y pudiendo prever si ciertos productos se venderán o no. Todo ello ha hecho más sencillo una parte del trabajo de las empresas (aunque tiene su contraparte en que esta tecnología está tan extendida que es accesible para las empresas en general, y no solo para aquellas más grandes). Cada día aparecen nuevas técnicas capaces de captar y tratar los datos de los usuarios.

Una de las más conocidas actualmente son las llamadas *cookies*, es decir, un texto alfanumérico que se descarga en el equipo (o bien terminal móvil), del destinatario de una prestación de un servicio de la sociedad de la información, cuya función es almacenar datos en el mismo que pueden ser recuperados en un momento posterior por el prestador del servicio cuando el destinatario vuelve a solicitar la información[117]. Pongamos un

[116] MARTÍNEZ PASTOR, E., "La publicidad comportamental *on line* y la protección de datos personales" en VALERO TORRIJOS, J. (Coord.), *La Protección de los Datos …,* cit. pág. 291. Si se busca una definición de qué es la publicidad comportamental, nos encontramos que el GT 29 la ha definido en su Dictamen 2/2010, de 22 de junio de 2010, definiéndola como "aquella publicidad que se basa en la observación continuada del comportamiento de los individuos" (pág. 5). Sin embargo, PÉREZ BES, discrepa de la definición dada por el GT 29, en tanto se centra en las técnicas que permiten individualizar a un usuario (en el dictamen), mientras que para él la publicidad comportamental supone "aquella publicidad que se muestra durante una concreta navegación, por razón de la actividad online que se ha venido desarrollando durante un periodo de tiempo determinado, desde ese mismo navegador" en PÉREZ BES, F., *La publicidad comportamental online,* UOC, Barcelona, 2012. Se empleará aquí la definición dada por MARTÍNEZ PASTOR.

[117] NAVAS NAVARRO, S., "*Cookies* y tecnología análoga: publicidad comportamental online y protección de los datos de carácter personal" en NAVAS NAVARRO, S., CAMACHO CLAVIJO, S., *Mercado Digital. Principios…*, cit. pág. 356. Sin embargo, conviene matizar que no son virus en sentido estricto. VÁZQUEZ RUANO pone como ejemplo comparativo la existencia de los "troyanos", programas parásitos que se alojan en el ordenador y cuya finalidad es causar daño con consecuencias destructivas,

ejemplo práctico: viendo determinada página web, una vez que he hecho clic en un producto o servicio que me interesa eso es almacenado en la *cookie* de mi ordenador y enviado como información a la empresa, de tal forma que en las siguientes visitas aparecerán más ofertas relacionadas con esos productos o servicios que previamente me han interesado. También puede ser que aparezcan ofertas de productos relacionados con los que yo he mirado en los *banners* (definidos en nota al pie 21) publicitarios alojados, por ejemplo, en el periódico que sigo normalmente.

Dentro de este tipo de programas, encontramos que existen las *cookies* anónimas, que no incluyen un campo identificador único para cada usuario[118]. Éstas, atendiendo al concepto de dato personal y su requerimiento de hacer al usuario identificable, no supondrían un problema siempre que estuviera legitimada la recogida de datos. El problema lo suponen las *cookies* identificativas: aquellas que sí incluyen un identificador único para cada usuario, y que permiten relacionar los accesos de usuario y crear perfiles más completos. Por último, aparecen un tipo de programas, llamadas *cookies* en flash, que se almacenan en el disco duro del ordenador a través de aplicaciones de flash (imágenes variables en las páginas web, típicamente los anuncios) al visitar un determinado sitio web. Éstas últimas suponen mayor problema: no son gestionables por el usuario (cosa que sí se puede realizar con los otros dos tipos, borrando desde el historial las *cookies*), por lo que es imprescindible informar al usuario de su instalación[119].

Estos programas, aunque no regulados específicamente por la normativa europea, sí que aparecen en los considerandos de la Directiva 2002/58 sobre privacidad y comunicaciones comerciales y también en los de la RGPD (sin mención en la DPD). En la primera, los considerandos 24 y 25 indican que si bien son instrumentos de gran utilidad para analizar determinadas características (desde el punto de vista de la empresa), éstos han de reunir determinadas características para ser lícitamente instaladas en los terminales: que la recogida de datos se haga con propósitos legítimos, informar de su uso a la persona y, además, solicitar el consentimiento del afectado[120] (en el art. 5.3 de la directiva 2002/58 también se apunta a estos requisitos para las "redes de comunicaciones electrónicas con fines de almacenamiento de información o de obtención de acceso a la información almacenada en el equipo terminal"). En el RGPD es el considerando 30 el que se refiere a las *cookies*, simplemente para indicar que son programas que permiten identificar a las personas y elaborar perfiles, indicando así que los datos recogidos por

pero que también recaba información de los ordenadores. La finalidad de las *cookies* es funcionar como herramientas útiles para entidades empresariales con diversos fines: controles de audiencia, identificación de usuarios para futuros envíos de publicidad, etc. en VÁZQUEZ RUANO, T., *La protección de los destinatarios de las comunicaciones comerciales electrónicas*, Marcial Pons, Madrid, 2008, pág. 162-164.

[118] PANIZA FULLANA, "Protección de datos, *cookies…"*. cit. pág. 27.

[119] PANIZA FULLANA, , "Protección de datos, *cookies…"*. cit. pág. 27.

[120] PEGUERA POCH, M., "Publicidad *online* basada en comportamiento y protección de la privacidad", RALLO LOMARTE, A., MARTÍNEZ MARTÍNEZ, R., *op. cit.* pág. 369-370.

estos programas entran dentro de la categoría de datos personales protegidos, puesto que hacen identificable al usuario.

En el caso de la normativa española, la LOPD no regula las *cookies*. Será la LSSICE en su art. 22.2 donde encontramos regulados los "dispositivos de almacenamiento y recuperación de datos en equipos terminales"[121] y la necesidad de que el afectado tenga información "clara y completa" sobre la utilización y finalidad de almacenamiento, habiendo prestado su consentimiento después de recibir esta información. Añade, además, que se le ha de ofrecer un procedimiento de oposición sencillo y gratuito. Respecto al consentimiento que ha de dar el usuario, no solo se trata de un consentimiento que se da ante un requerimiento de la empresa, sino que, además, en la mayoría de los casos se trata de un sistema de *opt-out*: si el usuario no quiere que se recopilen sus datos para recibir anuncios personalizados tendrá que manifestar su voluntad en ese sentido[122].

Toda esta regulación contiene un matiz (el art.5.3 de la Directiva 2002/58 sobre privacidad y comunicaciones comerciales y el art 22.2 LSSICE) por el cual todo lo establecido anteriormente (la información y el consentimiento) "no impedirá el posible almacenamiento o acceso de índole técnica al solo fin de efectuar o facilitar la transmisión de una comunicación a través de una red de comunicaciones electrónicas, o en la medida de lo estrictamente necesario a fin de proporcionar a una empresa de información un servicio expresamente solicitado por el usuario o el abonado". Se puede vislumbrar en estas líneas la posible "vía de escape" de las empresas (por ejemplo, aquellas que permiten las comunicaciones como son *Hotmail* o *Whatssap*) para almacenar información de los usuarios.

Una vez hemos definido la normativa y el concepto de las *cookies*, surgen los roces con la normativa de protección de datos: ¿pueden considerarse los datos que se recogen "dato de carácter personal"? ¿Puede supeditarse el acceso a determinados contenidos de un sitio web a la aceptación de las *cookies*? ¿qué fines se le da a esa información y cuáles son legítimos?

En cuanto a la primera cuestión, la definición adoptada primero por lo considerado por el GT 29 (ampliando y aclarando los conceptos de la DPD y LOPD[123]) y, a partir de mayo de 2018, por el RGPD, que incluye en su considerando 30 las *cookies* como elementos que identifican a la persona, no deja lugar a dudas: sobre todo las *cookies* no anónimas

[121] En esta fórmula tienen cabida las técnicas como las *cookies* entre otras. PANIZA FULLANA, , "Protección de datos, *cookies…".* cit. pág. 35.

[122] PEGUERA POCH, M., "Publicidad online basada en comportamiento…", cit. pág. 376.

[123] Vid. 2.2.1.- "Persona identificada o identificable" pág. 7.

permiten de forma inequívoca identificar a la persona, de tal forma que todo aquello que recoja será dato personal protegido.

En cuanto a la supeditación del acceso a determinados contenidos a la aceptación de dichos programas, el considerando 25 de la Directiva 2002/58 sobre privacidad y comunicaciones comerciales establece al final: "No obstante, se podrá supeditar el acceso a determinados contenidos de un sitio web a la aceptación fundada de un "chivato" (*cookie*) o dispositivo similar, en caso de que éste tenga un propósito legítimo". Ello hace necesario unirlo con la finalidad legítima en general de las *cookies*, respondiendo de forma conjunta a las dos preguntas.

Respecto a los fines legítimos, se entiende por fin legítimo[124] un objetivo justificado. Aunque esta condición es exigida por las distintas regulaciones, no se interpreta cuáles son los fines legítimos. Sí que establece el art. 4.2 LOPD aquellos que están excluidos de los fines incompatibles: fines históricos, estadísticos o científicos. Por tanto, al no contemplar específicamente los fines publicitarios, no se puede entender que es un fin legítimo para obligar a la aceptación de las *cookies* para acceder al sitio web.

No obstante, pueden surgir diferencias a la hora de establecer fines legítimos entre las *cookies* temporales o de sesión y las permanentes[125], en cuanto vinculan de forma permanente o no al usuario al envío de información, aunque ello no se contempla en la legislación actual. Mientras que los primeros únicamente recaban información cuando el usuario está visitando el sitio web desde el que se envían, eliminándose en el momento en el que se cierra el navegador (pudiendo responder así a un fin legítimo, como comprobar determinados datos), los segundos no tienen "caducidad", siendo ésta determinada por la empresa que los remite[126]. Pensemos en dos fines más o menos coherentes: si lo que se pretende es la identificación de las partes, con el fin de realizar una transacción, esta identificación tendrá un fin: en el momento en el que ambas partes cumplan las obligaciones contraídas, el archivo dejará de tener un fin legítimo y deberá ser eliminado. Sin embargo, si la finalidad del programa es verificar la efectividad de la estructura de su página o de las técnicas publicitarias que contiene, el plazo de duración puede ser indeterminado. Ello marca un matiz importante de temporalidad que quizá

[124] La LOPD (Art. 4.1) define la finalidad como explícita, determinada y legítima. Debe estar fijada con anterioridad a la recogida de datos. La legitimidad tiene su límite en la Constitución y en la ley, admitiéndose prácticamente cualquier finalidad. En REBOLLO DELGADO, L., SERRANO PÉREZ, M.M., *Manual de Protección…,* cit. 137-138.

[125] El GT 29 en su Dictamen 1/2008, de 4 de abril de 2008, estableció que "La utilización de *cookies* permanentes o de dispositivos similares con una ID de usuario única perite el seguimiento de los usuarios de un ordenador incluso cuando se utilizan direcciones IP dinámicas. Los datos de comportamiento que se generan mediante la utilización de estos dispositivos permiten centrarse más en las características personales de la persona en cuestión". Pág. 14.

[126] VÁZQUEZ RUANO, *op. cit.* pág. 182.

debería también ser tenido en cuenta por el legislador: el uso para fines puntuales o permanentes, que recaben los datos de forma continua y extendida en el tiempo.

Así, nos podemos preguntar: ¿Hay alguna forma de que las *cookies* no se instalen en mi ordenador? Si bien se pueden borrar las *cookies* ya instaladas, este acto solo tendrá efecto temporal: al volver a acceder a la página o sitios asociados a la red de publicidad, se volverán a instalar los programas. Una forma es la instalación de una "*opt-out cookie*" es decir, un programa que informa a la red publicitaria de que dicho ordenador ha decidido rechazar la *cookie* de publicidad (enviando ese rechazo posterior que permiten algunas páginas). Aun así, si el usuario decide borrar las *cookies* o inicia una navegación anónima, la red ya no le reconocerá y volverá a enviarlas. Hay navegadores, como Google, que permiten instalar un plug-in para guardar de modo permanente la opción de no recibir estas *cookies*[127]. También encontramos los bloqueadores de anuncios y *cookies*, que funcionan como informadores del no consentimiento (vid. apartado 4.4, donde quedaba definido)[128].

Sin embargo, las técnicas avanzan de forma muy rápida, de tal forma que hay nuevos programas (como las *cookies* en flash) que no son reconocidas[129] por estos programas anti-*cookies* y que hacen aún más difícil rechazar la instalación de programas que recaben nuestros datos.

5.2.- Creación de perfiles

Uno de estos usos relacionados con la publicidad comportamental es la creación de perfiles que, definido por la Agencia Europea de los Derechos fundamentales consiste en "categorizar a individuos en función de sus características (tales como género, edad, hábitos y comportamientos)"[130].

Pero, ¿por qué puede suponer esta técnica de creación de perfiles un problema? Por la definición dada por la Agencia Europea, el problema no se especifica. Sin embargo, el desarrollo de las técnicas de *Big Data* permite aunar todas esas características para crear perfiles que se convierten en instrumentos de decisión comercial (generalmente

[127] Además, la *Network Advertising Initiative* (NAI), ha desarrollado un sistema que permite inhabilitar las *cookies* de publicidad de múltiples redes publicitarias de modo conjunto. En VÁZQUEZ RUANO, *op. cit.* pág. 377.

[128] Si el punto de vista cambia, los bloqueadores de anuncios son vistos por la industria como un auténtico peligro para el modelo de negocio que se ha impuesto para los contenidos en internet ya que no permiten rentabilizar las páginas web. VEGA, Guillermo, "Publicidad. Bloqueadores de anuncios: ¿el fin de internet?, *El País*, 6 de Mayo de 2017.

[129] PANIZA FULLANA, "Protección de datos, *cookies…".* cit. pág. 54.

[130] Informe de la Agencia Europea de los Derechos fundamentales, "Understanding and preventing discriminatory ethnic profiling", glosado en GIL, E., *Big Data, privacidad…,* cit. pág. 124.

automatizadas), que detectan los mejores destinatarios de una oferta o, por el contrario, a los clientes indeseables[131]. En el sector del marketing basarse en perfiles para tomar decisiones puede tener "poco impacto": un error en la valoración del perfil de un cliente puede llevar simplemente a que un consumidor vea un anuncio u oferta que no le interesa, y un acierto a un aumento de las ventas. El verdadero problema de la creación de perfiles se muestra al usar estas técnicas en otros sectores: asegurador (aumentando el precio del seguro porque una persona sea fumadora, ya que tiene un riesgo más alto de padecer problemas de salud); o el bancario, pudiendo saber de forma más certera si la persona pertenece, por sus características, a los grupos más fiables que devuelven los préstamos o no. Sin embargo, sí es un problema generalizado que se tomen decisiones (incluso sobre anuncios u ofertas) basándose en características que pueden llevar a decisiones discriminatorias[132] (raza, género, etc.).

El Dictamen 2/2010 sobre publicidad comportamental *on-line*, de 22 de junio de 2010, ha indicado que hay dos tipos de perfiles: los predictivos que se establecen por la observación continuada del comportamiento en línea de los usuarios siguiendo las páginas web que visitan y los anuncios que seleccionan; y los explícitos, que se crean a partir de los datos de carácter personal que los usuarios proporcionan. Una de las formas de conseguir todos estos datos son las *cookies*[133].

Por ello, la LODP regula en su art. 13 estas decisiones, dando a la persona el "derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad". Así, por ejemplo, la Instrucción 2/1995, de 4 de mayo, de la AEDP indicó que se amparaba bajo la prohibición de este precepto que se denegara un préstamo bancario por los datos obtenidos en el seguro de vida obligatorio. No importa la veracidad de la información incorporada al perfil, sino que éste sea el único fundamento para adoptar la decisión (sin ponderar otros factores)[134].

En cuanto a la regulación europea, la DPD regula en su art. 15.1 las decisiones individuales automatizadas de la misma forma que la LOPD en su art. 13. Sin embargo, a diferencia de la LOPD, en su apartado 2 establece dos excepciones a este derecho: que esta decisión se haya adoptado en el marco de la celebración o ejecución de un contrato (en determinadas condiciones) o que la decisión este autorizada por una ley que establezcan medidas que garanticen el interés legítimo del interesado. En cuanto al RGPD, regula en su art. 22 este tratamiento, definiéndolo de igual forma que la anterior

[131] LLÁCER MATACÁS, M.R., *La autorización al… cit.* pág. 38.
[132] El acto de discriminación representa un trato desfavorable aplicado a situaciones comparables y no amparado en un fin legítimo. En LLÁCER MATACÁS, M.R., *La autorización al… cit.* pág. 39.
[133] NAVARRO, S., "*Cookies* y tecnología análoga…" cit. pág. 366.
[134] LLÁCER MATACÁS, M.R., *La autorización al… cit.* pág. 41.

normativa, pero añadiendo una excepción más que la DPD a que se aplique el derecho a no ser objeto de una decisión basada únicamente en el perfil: el consentimiento expreso del interesado. Además, añade en su art. 22.4 RGPD refuerza la protección de las categorías especiales del art. 9, estableciendo que las excepciones del art. 2 no se aplican para éstos (conformando así una excepción de la excepción).

5.3.-Uso de los datos y la licitud de la cesión a terceros. Especial referencia a herramientas publicitarias.

No es raro que, en las condiciones sobre datos personales que incluyen las empresas, encontremos referencias a que esos datos pueden ser tratados por terceros que no son directamente con los que se tiene relación. En muchos casos, son las empresas con las que se tiene relación (utilizando su app, su página web o determinados servicios) las que venden a terceras empresas los datos que recaban de los usuarios de sus páginas (de ahí que exista actualmente toda una industria del tratamiento de datos). Por ejemplo, es una de las formas de las que se nutrían las empresas de *Spam* para recabar cuentas de correo de usuarios a las que, posteriormente, mandar correos publicitarios. En este apartado veremos la regulación de la cesión de datos y también la del fenómeno conocido como *Spam*, y su relación con la protección de datos.

5.3.1.- La cesión de datos.

La venta de los datos de unas empresas a otras requiere que los responsables[135] de los datos cedan o comuniquen los datos a estas terceras empresas. Curiosamente, esta cesión o comunicación de los datos sólo se regula en la LOPD y su reglamento de desarrollo, siendo omitida completamente tanto por la DPD[136] como por el nuevo RGPD, que las consideran una posibilidad dentro de la actividad general de tratamiento. La cesión o comunicación de datos se define en el art. 3.i. LOPD como "toda revelación de datos realizada a una persona distinta del interesado", complementándose en el art. 5.1.c. RLOPD que la define como "Tratamiento de datos que supone su revelación a una persona distinta del interesado". Este matiz introducido por el reglamento de desarrollo

[135] El RGPD diferencia, en su art. 4 entre "responsable del tratamiento" y el "encargado del tratamiento". Mientras el primero es la "persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento" (art. 4.7), el segundo, el encargado, es "la persona física o jurídica, autoridad pública, servicio u otro organismo que trate los datos personales por cuenta del responsable del tratamiento" (art. 4.8). Esta segunda figura se regula en el art. 28 RGPD.

[136] La DPD hace referencia a la cesión o comunicación de datos como un supuesto del tratamiento de datos, en su art. 2.b. cuando hace referencia a su "comunicación por transmisión". En MESSÍA DE LA CERDA BALLESTEROS, J.A., *op. cit.* pág. 68. Del mismo modo lo realiza el RGPD, en su art. 4.2

es importante ya que así se implican todas las operaciones que puedan hacerse con los datos[137] y que quedan englobadas en la noción de tratamiento[138].

Su régimen se regula en el art. 11.1 LOPD, indicando que solo podrán ser comunicados a un tercero "para el cumplimiento de los fines directamente relacionados con las funciones del cedente y del cesionario con el previo consentimiento del interesado". De nuevo, el consentimiento es el principal mecanismo de protección de los datos personales[139]. El consentimiento para la cesión ha de tener los mismos requisitos que el consentimiento para la recogida y tratamiento de datos (vid. apartado 4).

Hay, no obstante, ciertas situaciones en las que el consentimiento no es necesario. De un lado, el art. 11.6 LOPD establece que no se aplicará el régimen de los apartados anteriores (entendiéndose, la necesidad de recabar el consentimiento) en el caso en el que los datos estén disociados, es decir, que no permitan la identificación de un afectado o interesado[140]. Existen además, excepciones legales al consentimiento, establecidas en el art. 11.2 LOPD: la cesión autorizada por una ley; cuando se trate de datos recogidos de fuentes accesibles al público; cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros (por la existencia de una relación jurídica que se acepta de forma voluntaria)[141]; cuando la comunicación se efectúe por el Defensor del Pueblo, al Ministerio fiscal o los Jueces o Tribunales o el Tribunal de cuentas, en ejercicio de sus funciones; cesión entre Administraciones públicas y con finalidades históricas, estadísticas o científicas; o, por último, por motivos sanitarios (como solucionar una urgencia que requiera acceder a un fichero o estudios epidemiológicos).

De igual forma que la recogida y tratamiento de los datos, el consentimiento dado para la cesión o comunicación de los datos tiene carácter revocable, según el art. 11. 4 LOPD.

Hay que indicar que diferente a la cesión, definida en el art. 11 LOPD, es el acceso a los datos por cuenta de terceros, regulado en el art. 12 LOPD y que actualmente recibe el nombre de *outsourcing*[142]. Esta relación se puede definir como la externalización de

[137] REBOLLO DELGADO, L., SERRANO PÉREZ, M.M., *Manual de Protección…,* cit. 155.
[138] El tratamiento se define en la LOPD en su art. 3.c. como "operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias".
[139] Siendo nulo ese consentimiento si no se ha informado sobre la finalidad de los datos. PANIZA FULLANA, , "Protección de datos, *cookies…".* cit. pág. 49.
[140] La definición de dato disociado y procedimiento de disociación se definen en el art. 5 del RLOPD.
[141] REBOLLO DELGADO, L., SERRANO PÉREZ, M.M., *Manual de Protección…,* cit. 160.
[142] MESSÍA DE LA CERDA BALLESTEROS, J.A., *op. cit.* pág. 163.

servicios pertenecientes a una empresa fuera de la misma, cediendo su gestión a otras sociedades[143]. Es una práctica común en la sociedad actual en las empresas, que no tienen desarrolladas determinadas áreas (comúnmente áreas informáticas o jurídicas[144]) y que subcontratan los servicios dados por otras empresas[145]. Ésta figura tiene una regulación específica dentro de la LOPD. Por lo tanto, son diferentes las situaciones de cesión, por la cual los datos se utilizan en posible beneficio de una tercera empresa, de *outsourcing*, en las cuales, por falta de medios o departamentos especializados, la empresa cede los datos a otra para realizar un tratamiento para la primera.

En este ultimo tipo de contrato, cobra especial importancia la exigencia del contrato (art. 12.2 LOPD), ya que este deberá establecer las instrucciones para el tratamiento de los datos y sus fines, prohibiendo de forma expresa la aplicación o cesión de esos datos por parte del tercero con fines distintos de los establecidos en el contrato, de tal forma que si estas condiciones se incumplen, se especifica en el art. 12.4 la responsabilidad del tercero: en caso de que use los datos para otra finalidad o los ceda, será considerado también responsable del tratamiento, respondiendo de las infracciones correspondientes[146]. En cuanto al uso de los datos personales una vez la relación entre las empresas ha concluido, el art. 12.3 establece que éstos habrán de ser destruidos o devueltos al responsable del tratamiento.

5.3.2.- La problemática del *Spam.*

El correo electrónico constituye una importante, aunque ya no novedosa, herramienta publicitaria, que ha sido utilizado por las empresas con el fin de acercar sus productos y servicios a las personas[147]. Uno de sus usos ha sido para enviar el conocido como *Spam*, es decir, envío de publicidad, normalmente con carácter masivo, no solicitada por medios electrónicos[148] (donde se pueden englobar también los enviados por SMS o MMS, aunque sigue siendo preponderante el uso del correo electrónico). Esta publicidad es, para el

[143] La Subcontratación es la técnica de gestiónempresarial consistente en la externalización, total o parcial, de las necesidades que con anterioridad venían siendo desarrolladas en el seno de la propia organización (o podrían haberlo sido). Este tipo de relación suele ser cedida por un tiempo largo (entre 5 y 10 años) y a cambio de un precio. En APARICIO VAQUERO, J.P. *La nueva contratación informática. Introducción al Outsourcing de los Sistemas de Información*, Editorial Colmares, Granada, 2002, pág. 23.

[144] Aunque en su origen este tipo de contrato no se refiere al uso de la tecnología para el tratamiento de la información, la importancia adquirida por este caso hace que el uso de este contrato sea por excelencia el informático. En APARICIO VAQUERO, J.P. *op. cit.* pág. 15.

[145] Aparece así la figura del "encargado" del tratamiento, diferente al del responsable, que se puede definir como la persona (jurídica, física o AAPP) que solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento. REBOLLO DELGADO, L., SERRANO PÉREZ, M.M., *Manual de Protección…,* cit. 164.

[146] Esta exigencia es imperativa, de tal forma que ni siquiera con el consentimiento del afectado el tercero podría proceder a la cesión de datos. Así, esta norma se esfuerza en evitar abusos de la información que se gestiona en virtud de estos contratos. MESSÍA DE LA CERDA BALLESTEROS, J.A., *op. cit.* pág. 171-173.

[147] JIMÉNEZ, D., *op. cit.* págs. 489-490.

[148] TATO PLAZA, A., "Aspectos jurídicos del Spam" en FERNÁNDEZ LÓPEZ, *op. cit.* pág. 55.

empresario, una forma de contacto con consumidores dispersos muy rápida y relativamente barata. Todo ello, unido a la publicidad comportamental, que permite crear perfiles del consumidor, posibilita que estos correos se dirijan únicamente a destinatarios que, en un principio, podrían estar interesados en el producto o servicio promocionado. Para el consumidor, estos envíos pueden llegar a resultar pesados y abusivos[149].

La normativa europea que regula el *Spam* la encontramos en la Directiva 2002/58 sobre privacidad y comunicaciones comerciales, cuyo art. 13.2 indica, cuando una empresa ha obtenido de sus clientes el correo electrónico: "podrá utilizar dichas señas electrónicas para la venta directa de sus propios productos o servicios de características similares, a condición de que se ofrezca con absoluta claridad a los clientes, sin cargo alguno y de manera sencilla, la posibilidad de oponerse a dicha utilización de las señas electrónicas en el momento en que se recojan las mismas y, en caso de que el cliente no haya rechazado inicialmente su utilización, cada vez que reciba un mensaje ulterior". Esta normativa fue incorporada al ordenamiento español por la LGT, que introdujo la modificación de los artículos 21 y 22 de la LSSICE. Así, el ordenamiento español exige para el envío de comunicaciones publicitarias el consentimiento de los destinatarios. El *Spam* se encuentra sancionado por la Ley de Competencia Desleal, en su art. 29[150] siendo configurada como una práctica agresiva por acoso las "propuestas no deseadas y reiteradas por teléfono, fax, correo electrónico u otros medios de comunicación a distancia" (aunque esta última no pretende la protección de los datos personales, sino del mercado).

El consentimiento exigido por la LSSICE en su art. 21 es expreso, a diferencia de lo visto con el consentimiento general de la protección de datos. Así, esta práctica requiere de un sistema de consentimiento *opt-in*[151] es decir, de declaración previa. Este consentimiento expreso tiene una excepción, regulada en el art. 21.2, cuando exista una relación contractual previa y la publicidad se refiera a productos o servicios similares que los que fueron objeto de contratación previa (de lo que se presume que existe consentimiento previo)[152]. Este consentimiento, además, ha de ser revocable de forma sencilla (art. 22.1).

Además del consentimiento, la LSSICE exige, en su artículo 20, que estas prácticas sean identificadas como publicitarias y que se identifique a la persona física o jurídica que realiza la comunicación. La exigencia de la identificación de publicidad dentro del mensaje, si bien resulta útil, puede resultar insuficiente ya que requiere del destinatario que abra el mensaje, por lo que sería preferible que se exigiera un código identificativo en el título o asunto del mensaje. En cuanto a la identificación de la entidad que realiza la

[149] DRUMMOND, V., op. *cit.* pág. 77.
[150] Que recoge lo establecido en la Directiva 2005/29/CE, de 11 de mayo, sobre prácticas comerciales desleales de las empresas en sus relaciones con los consumidores, en el apartado 26 de su anexo.
[151] VÁZQUEZ RUANO, *op. cit.* pág. 328.
[152] TATO PLAZA, *op. cit.* pág. 61.

comunicación, tiene sentido por la necesidad de tener constancia del responsable a los efectos de exigencia de responsabilidad.

Toma especial relevancia en cuanto a este trabajo se refiere, la relación que hay entre el *Spam* y la normativa de protección de datos, ya que las campañas publicitarias de este tipo implican la utilización de datos de carácter personal. Así, la LSSICE recuerda, en su art. 19.2 la plena aplicación de la LOPD a este tipo de prácticas. Esto hace que el envío de publicidad electrónico sólo sea lícito si, además de cumplir los requisitos exigidos para el *spam*, se respeten las normas vistas anteriormente sobre la obtención y tratamiento de datos establecidos en la normativa de protección de datos personales[153]. Así, se puede ver que en el art. 30 LOPD se exige que "quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial y otras actividades análogas, utilizarán nombres y direcciones u otros datos de carácter personal cuando los mismos figuren en fuentes accesibles al público o cuando hayan sido facilitados por los propios interesados u obtenidos con su consentimiento".

De esta forma, al margen de las fuentes accesibles al público, nos surge la duda de si el consentimiento dado para el envío de publicidad por correo electrónico (expreso) equivale o suple al consentimiento para el tratamiento del dato personal[154]. Lo establecido en la LOPD sobre el consentimiento, en especial la necesidad de que éste sea expreso para el tratamiento de datos personales nos responde a la duda: el consentimiento dado por la persona para recibir el *Spam* no exime al anunciante de recabar el consentimiento necesario para la obtención y tratamiento de datos personales.

[153] TATO PLAZA, *op. cit.* pág. 65-67. Sin embargo, VÁZQUEZ RUANO (VÁZQUEZ RUANO, *op. cit.* pág.338) indica que la relación entre la LOPD y la LSSICE no es tan clara: hay autores que consideran que, en materia de protección de datos en Internet la LOPD debe adaptarse a la LSSICE (como considera TATO PLAZA), de tal forma que el consentimiento debe ser diferente para la obtención de datos, de un lado, y para el envío de publicidad, de otro. Sin embargo, hay otros autores que consideran que la LOPD es especial (aplicando el principio de ley especial prima sobre ley general) respecto a la LSSICE, por lo que el consentimiento para tratar los datos implicaría el consentimiento para enviar *Spam*. En mi opinión, la LSSICE añade el matiz del uso de los datos en el contexto de internet, un contexto específico dentro de los que se puede mover la protección de datos, por lo que se ha adoptado la tesis de TATO PLAZA.

[154] TATO PLAZA, *op. cit.* pág. 67.

6.- Conclusiones

Del estudio realizado acerca del derecho a la protección de datos y las herramientas publicitarias a lo largo del Trabajo Fin de Grado, puedo extraer las siguientes conclusiones:

I. **Importancia creciente del derecho a la protección de datos y desinformación del usuario.** El aumento del valor económico de la información, unido al incremento de las posibilidades de vulneración de los datos personales de los individuos, ha conllevado el incremento de la preocupación del legislador por configurar el derecho a la protección de datos. Importancia de la protección de datos teórica para el individuo: se preocupa por sus datos, pero rara vez toma medidas (como leer las condiciones) para informarse y protegerlos.

II. **Definición amplia de dato personal.** La evolución de las técnicas de recogida y tratamiento de datos personales (*Big Data*, *Cookies*, etc.) ha hecho necesaria la configuración de una definición amplia de dato personal, que incluya cualquier tipo de dato siempre y cuando éste permita la identificación (de forma individual o mediante el tratamiento de un conjunto de datos) del individuo.

III. **Insuficiencia del consentimiento y auge de nuevos mecanismos de control.** Las prácticas utilizadas por las empresas para recabar el consentimiento hacen que este mecanismo revele su insuficiencia como eje vertebrador de la protección de datos, a pesar de su refuerzo y aclaraciones conceptuales realizados en la nueva normativa de la Unión Europea (RGPD). Crece la importancia de los nuevos mecanismos de control de datos personales, que se acercan a un sistema de autocontrol por parte de las empresas y también por el mercado (sistemas de certificación).

IV. **Desarrollo de las técnicas de recogida de datos e influencia en la protección de datos.** El desarrollo de programas como las *cookies*, unido a la tecnología del *Big Data*, hacen que los usuarios sean identificados de forma más sencilla. Estos datos son usados por las empresas para diversos fines, aunque uno de los más extendidos es el de ofrecer al consumidor publicidad personalizada.

V. **Necesidad de informar al usuario y recabar su consentimiento para la instalación de *cookies*. Dudosa licitud de supeditar el acceso a una página determinada al consentimiento de instalación de las *cookies*.** La normativa de protección de datos obliga a las empresas que gestionan las páginas web a recabar el consentimiento del usuario, si bien con un sistema *opt-out*: presumiendo el consentimiento por seguir navegando en la página correspondiente y dándole un

plazo para negarse al uso de los programas. Ello lleva a que muchas páginas subsuman el acceso a la página a aceptar las *cookies*, escudándose en el argumento de que lo realizan con un propósito legítimo. En la práctica, son patentes las dificultades para encontrar maneras de rechazar las *cookies.*

VI. **Los perfiles de los usuarios, una herramienta con condiciones.** la toma de decisiones automatizadas basadas en determinadas características de la personalidad no será posible, a menos que se encuadre en una relación contractual, esté autorizada por ley o, a partir de la aplicación del RGPD, se cuente con el consentimiento del usuario. Esta creación de perfiles se regula porque, aunque resulta muy útil para las empresas, puede tener consecuencias discriminatorias para la persona.

VII. **Regulación española de la cesión de datos, condicionada al consentimiento de la persona y siempre en cumplimiento de los fines buscados por la empresa que cede los datos.** Llama la atención que la cesión de datos, como figura autónoma, sólo se contempla en la legislación española (LODP y RLODP), quedando como una parte del tratamiento en el RGPD (y por tanto no incrementando los requisitos para su válida realización por parte de las empresas). De nuevo nos encontramos con una actividad que requiere el consentimiento del interesado (aunque con excepciones). Importante no confundir la figura de la cesión de datos con el *outsourcing*, que es la externalización de las funciones informáticas de una empresa y, por tanto, del tratamiento de datos.

VIII. **Necesidad de consentimiento expreso, y diferenciado del consentimiento para el tratamiento de datos, para la recepción del *Spam*.** Con una regulación extensa tanto en Derecho europeo como español, esta práctica publicitaria requiere del consentimiento expreso del destinatario para ser lícita con una excepción: la existencia de relación contractual entre remitente y destinatario. En su relación con la protección de datos, el correo se configura como un dato personal (vid. apartado 2.2.1) y es distinto el consentimiento que se da para enviar esos correos publicitarios que el que se da para que la información que pudiera recabarse de los mismos se recoja y trate como datos personales.

IX. **En general, dificultad de regulación de la protección de datos personales, con un marco normativo complejo y problemático a la hora de seguir vigente.** El binomio de datos personales y tecnología (en particular, internet), hace muy difícil la tarea del legislador. El marco normativo es complejo y diverso, por la multitud de normas que influyen y regulan las relaciones ocurridas en Internet. Además, se ve necesaria una revisión recurrente y periódica de las condiciones que configuran

el Derecho a la Protección de Datos Personales en relación con los nuevos programas informáticos y las nuevas técnicas publicitarias, para actualizarlas a las necesidades de los usuarios.

7.- Bibliografía

- AGUADO, J.M., "La publicidad como problema. El impacto de los bloqueadores de anuncios en la industria del contenido digital", *Telos: Cuadernos de comunicación e innovación,* nº 103, 2016, págs. 6-9.

- APARICIO VAQUERO, J.P. *La nueva contratación informática. Introducción al Outsourcing de los Sistemas de Información,* Editorial Colmares, Granada, 2002.

- ANDREU MARTINEZ, M.B., PLANA ARNALDOS, M.C, "El poder de disposición del titular como facultad principal del derecho a la protección de los datos personales: su efectividad en el actual escenario tecnológico" VALERO TORRIJOS, J. (Coord.), *La protección de los Datos Personales en Internet ante la Innovación Tecnológica. Riesgos, Amenazas y respuestas desde la perspectiva jurídica,* Aranzadi, Pamplona, 2013, págs. 131-151.

- BLASI CASAGRAN, E., "La protección de datos en las aplicaciones de mensajería instantánea", VALERO TORRIJOS, J. (Coord.), *La protección de los Datos Personales en Internet ante la Innovación Tecnológica. Riesgos, Amenazas y respuestas desde la perspectiva jurídica,* Aranzadi, Pamplona, 2013, págs. 543-564.

- BUREAU VERITAS FORMACIÓN, *Ley de protección de datos personales. Manual práctico para la protección de los datos personales de las personas físicas,* FC Editorial, Madrid, 2009.

- CÁMARA LAPUENTE, S., "El régimen de la falta de conformidad en el contrato de suministro de contenidos digitales según la Propuesta de Directiva de 9.12.2015", *Indret (Revista para el análisis del Derecho),* Barcelona, 2016.

- COLIN, C., PULLET, Y., "Sociedad de la información y Marketing: *case* study" en LLÁCER MATACÁS, M.R., *Protección de datos personales en la sociedad de la información y la vigilancia,* La Ley, Madrid, 2011, págs. 229-273.

- DRUMMOND, V., *Internet, privacidad y datos personales,* Ed. Reus, Madrid, 2009.

- GALÁN MUÑOZ, A., "¿Nuevos riesgos, viejas respuestas? Estudio sobre la protección penal de los datos de carácter personal ante las nuevas tecnologías de la información y la comunicación", en GALÁN MUÑOZ, A. (Coord.), La *protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y comunicación,* Tirant lo Blanch, Valencia, 2014, págs. 203-279.

- GARCÍA PÉREZ, R.M., "La protección de datos de carácter personal del Consumidor en el Mercado Único Digital", *Revista de Derecho Mercantil*, julio-septiembre, 2016, págs. 199-249.

- GARRIGA DOMÍNGUEZ, A., *Nuevos retos para la Protección de datos personales*, Dykinson, Madrid, 2015.

- GIL GONZÁLEZ, E., "*Big data* y datos personales: ¿es el consentimiento la mejor manera de proteger nuestros datos?, Diario la Ley, Nº 9050, 2017.

- GIL GONZÁLEZ, E., *Big Data, privacidad y protección de datos*, Agencia Española de Protección de Datos, Madrid, 2016.

- HERRÁN ORTIZ, A., "La protección de datos personales de los consumidores y usuarios en los servicios de comunicaciones electrónicas" en CANEDO ARRILLAGA, M.P. (Coord.), *Derecho del Consumo: Actas del Congreso Internacional sobre Derecho de Consumo*, Tirant lo Blanch, Valencia, 2009, págs. 605-638.

- LLÁCER MATACÁS, M.R., *La autorización al tratamiento de información personal en la contratación de bienes y servicios*, Dykinson, Madrid, 2012.

- LÓPEZ JIMÉNEZ, D., "El denominado *bluespam*: incidencia sobre la privacidad del destinatario", VALERO TORRIJOS, J. (Coord.), *La protección de los Datos Personales en Internet ante la Innovación Tecnológica. Riesgos, Amenazas y respuestas desde la perspectiva jurídica*, Aranzadi, Pamplona, 2013, págs. 489-517.

- LÓPEZ JIMENEZ, D., CARLOS DITTMAR, E., "Internet móvil y geolocalización: nuevos retos para la privacidad en la era digital" VALERO TORRIJOS, J. (Coord.), *La protección de los Datos Personales en Internet ante la Innovación Tecnológica. Riesgos, Amenazas y respuestas desde la perspectiva jurídica*, Aranzadi, Pamplona, 2013, págs. 519-542.

- MAROTO CALATAYUD, M., "Redes sociales en Internet y "Data mining" en la prospección e investigación de comportamientos delictivos" en RALLO LOMARTE, A., MARTÍNEZ MARTÍNEZ, R., *Derecho y Redes sociales*, Civitas, 2010, págs. 207-257.

- MARTÍNEZ PASTOR, E., "La publicidad comportamental *on line* y la protección de datos personales", VALERO TORRIJOS, J. (Coord.), *La protección de los Datos Personales en Internet ante la Innovación Tecnológica. Riesgos, Amenazas y respuestas desde la perspectiva jurídica*, Aranzadi, Pamplona, 2013, págs. 291-306.

- MESSÍA DE LA CERDA BALLESTEROS, J.A., *La cesión o comunicación de datos de carácter personal*, Thomson Civitas, Madrid, 2003.

- MIRALLES, R., "El derecho a la portabilidad de los datos personales o prestaciones "premium" del tradicional derecho de acceso", VALERO TORRIJOS, J. (Coord.), *La protección de los Datos Personales en Internet ante la Innovación Tecnológica. Riesgos, Amenazas y respuestas desde la perspectiva jurídica*, Aranzadi, Pamplona, 2013, págs. 273-290.

- NAVAS NAVARRO, S., "Computación en la nube: Big Data y protección de datos personales", Indret (Revista para el Análisis del Derecho), Barcelona, nº4, 2015.

- NAVAS NAVARRO, S., "*Cookies* y tecnología análoga: publicidad comportamental online y protección de los datos de carácter personal" NAVAS NAVARRO, S., CAMACHO CLAVIJO, S., *Mercado Digital. Principios y reglas jurídicas*, Tirant lo Blanch, Valencia, 2016, págs. 357- 380.

- NAVAS NAVARRO, S., "El internet de las cosas" NAVAS NAVARRO, S., CAMACHO CLAVIJO, S., *Mercado Digital. Principios y reglas jurídicas*, Tirant lo Blanch, Valencia, 2016, págs. 27-61.

- OLIVER-LALANA, D., MUÑOZ SORO, J.F., "El mito del consentimiento y el fracaso del modelo individualista de protección de datos", VALERO TORRIJOS, J. (Coord.), *La protección de los Datos Personales en Internet ante la Innovación Tecnológica. Riesgos, Amenazas y respuestas desde la perspectiva jurídica*, Aranzadi, Pamplona, 2013, págs. 153-196.

- ORTEGA GIMÉNEZ, A., "La tutela del afectado ante los tratamientos ilícitos de sus datos personales desde la perspectiva internacional y su proyección en Internet" en VALERO TORRIJOS, J. (Coord.), *La protección de los Datos Personales en Internet ante la Innovación Tecnológica. Riesgos, Amenazas y respuestas desde la perspectiva jurídica*, Aranzadi, Pamplona, 2013, págs. 197-221.

- PANIZA FULLANA, A., "Protección de datos, *cookies* y otros instrumentos de navegación" en FERNÁNDEZ LÓPEZ, J.M., *Publicidad, Defensa de la Competencia y Protección de datos*, Thomson Reuters, Pamplona, 2010, págs. 25-54.

- PEGUERA POCH, M., "Publicidad *online* basada en comportamiento y protección de la privacidad", RALLO LOMARTE, A., MARTÍNEZ MARTÍNEZ, R. *Derecho y Redes sociales*, Civitas, 2010, págs. 355-380.

- PEGUERA POCH, M., "Servicios de la Sociedad de la Información" en PEGUERA POCH, M. (Coordinador), *Derecho y Nuevas Tecnologías,* Ed. UOC, Barcelona, 2005, págs. 141-190.

- PÉREZ BES, F., *La publicidad comportamental online,* UOC, Barcelona, 2012.

- PUENTE ESCOBAR, A., "Breve descripción de la evolución histórica y del marco normativo internacional del Derecho fundamental a la Protección de Datos de carácter personal" en PIÑAR MAÑAS, J.L. (Coord.), *Protección de datos de carácter personal en Iberoamérica (II Encuentro Iberoamericano de Protección de datos, La Antigua-Guatemala, 2-6 de junio de 2003),* Tirant lo Blanch, Valencia, 2005, págs. 37-67.

- REBOLLO DELGADO, L., "Protección de datos (I): Origen, Justificación de su necesidad y regulación en Europa", en REBOLLO DELGADO, L., GÓMEZ SÁNCHEZ, Y., *Biomedicina y Protección de Datos,* Dykinson, Madrid, 2009, págs. 121-142.

- REBOLLO DELGADO, L., SERRANO PÉREZ, M.M., *Manual de Protección de Datos,* Dykinson, Madrid, 2014.

- ROSSI CARLEO, L. "La sociedad de la Información: el ciudadano frente al poder de decisión ajeno" en LLÁCER MATACÁS, M.R., *Protección de datos personales en la sociedad de la información y la vigilancia,* La Ley, Madrid, 2011, págs. 23-38.

- SCHÜTZ, P., "The Set up of Data Protection Authorities as a New Regulatory Approach" en GUTWIRTH, S., LEENES, R., DE HERT, P., POULLET, Y. (Editors), *European Data Protection: In Good Health?* Springer, London, 2012.

- SERRANO PEREZ, M.M., *El Derecho Fundamental a la Protección de Datos. Derecho Español y Comparado,* Thomson, Madrid, 2003.

- SIMÓN CASTELLANO, P., *El régimen constitucional del derecho al olvido digital,* Tirant lo Blanch, Valencia, 2012.

- TATO PLAZA, A., "Aspectos jurídicos del Spam" en FERNÁNDEZ LÓPEZ, J.M., *Publicidad, Defensa de la Competencia y Protección de datos,* Thomson Reuters, Pamplona, 2010, págs. 55-76.

- VALERO TORRIJOS, J., "Las quiebras en Internet de la regulación legal del derecho a la protección de los datos de carácter personal: la necesaria superación de un modelo desfasado" en VALERO TORRIJOS, J. (Coord.), *La protección de los Datos Personales en Internet ante la Innovación Tecnológica. Riesgos, Amenazas y respuestas desde la perspectiva jurídica*, Aranzadi, Pamplona, 2013, págs. 25-63.

- VÁZQUEZ RUANO, T., *La protección de los destinatarios de las comunicaciones comerciales electrónicas*, Marcial Pons, Madrid, 2008.

- VEGA VEGA, J.A., *Contratos electrónicos y protección de los consumidores*, Editorial Reus, Madrid, 2015.

- VILASAU SOLANA, M., "Derecho a la intimidad y protección de datos personales" en PEGUERA POCH (Coordinador), *Derecho y Nuevas Tecnologías*, Ed. UOC, Barcelona, 2005, págs. 93-139.